Federal mandates to harness and protect government data more effectively are pressuring agencies to embrace identity-centric, zero-trust security practices over perimeter defense. But multi-factor authentication practices are also helping agencies accelerate moves to the cloud and more modern applications and devices.
Moving to an identity-centric, perimeter-less data environment

Recent federal government mandates — from the Federal Data Strategy action plan to the OPEN Government Data Act — are placing greater demands on agencies to use and protect government data more effectively.

At the same time, public and commercial enterprises recognize that perimeter defense tactics are no longer effective by themselves in protecting sensitive data from hackers and insider threats.

That’s prompted a wholesale shift in how organizations protect their data — from the inside out — and adopt a “zero-trust” approach to users and devices moving across their networks.

By surrounding their data with precision identity and access controls, agencies can better secure their information and improve the user experience for employees and citizens.

But moving to an identity-centric, perimeter-less data environment requires a combination of policy, investment and technology decisions.

FedScoop wanted to gain a clearer picture of how well federal agencies are in embracing this shift in approach and identify some of the key issues that leaders in the federal government IT community are facing.

“While hardening the perimeter is important, agencies must shift from simply managing access inside and outside of the perimeter to using identity as the underpinning for managing the risk posed by attempts to access federal resources made by users and information systems,”

White House FICAM memo »
In this new survey of federal agency and industry information technology decision makers, underwritten by Duo Security, FedScoop explored:

1. How far along federal agencies are in moving from a perimeter defense approach to a perimeter-less, “zero-trust” security model (which relies solely on managing device and user credentials to limit access to enterprise resources).

2. The extent to which agencies have developed a Federal Identity, Credential and Access Management (FICAM) strategy to meet White House OMB policy requirements and how that has impacted their security efforts.

3. How far along agencies are in inventorying and managing the identity of people and devices accessing their networks and applications.

4. What challenges are keeping agencies from adopting a zero-trust strategy.
Nearly half (48%) of federal government IT decision makers report their agency is substantially on their way to adopting an identity-focused approach to protecting access to agency resources.

But 3 in 10 government respondents say their agency still relies heavily on perimeter defense tools or policies.

50% of government respondents said their agency has a strategy to meet the White House OMB’s Federal Identity and Access Management (FICAM) policy requirements.

The further along agencies are to having a FICAM strategy, the more advanced they are in consolidating identity and access controls to agency resources.

Between 41 and 48 percent of respondents are still in the early stages of taking inventory of the people and/or devices accessing the organization’s networks.

Respondents indicated their organizations are moving towards a password-less user experience — with a little more than half planning to do so within the next two years.

Among various authentication options available to agencies, respondents ranked multifactor one-time password, randomly chosen password/PIN and out-of-band authenticators as their top three choices for where they plan to increase investments over the next two years.
FedScoop conducted an online survey of 171 prequalified government and industry IT decision makers about agency perceptions regarding identity verification capabilities. The survey was conducted in November 2019.

**Respondent by sector:**
- **Federal government:** 123 respondents
- **Industry/Govt. Contractors:** 48 respondents

**Respondent breakout by type of agency:**
- **Civilian Agency:** 57%
- **Defense Agency:** 25%
- **Other (research, contract, etc.)**: 18%

**Respondent breakout by job title:**
- **IT management:** 33%
- **Program / project management or staff:** 23%
- **C-suite/executive level IT decision-maker:** 17%
- **Cybersecurity management:** 8%
- **ICAM management or staff:** 3%
- **Other (analyst, administration, specialist):** 16%
Agency progress: Moving from perimeter defense to identity centric security

48% of federal government respondents — and 59% from government contractors and industry — say their agency/organization is on its way to adopting an identity-focused security approach.

However, 3 in 10 federal government respondents say their agency still relies heavily on perimeter defense tools or policies.

Federal Government Respondents
- Still relies heavily on perimeter defense tools / policies: 29%
- Is still evaluating tools to centrally manage identity / access to agency resources: 23%
- Has begun consolidation identity / access to agency resources: 20%
- Has mostly consolidation identity / access to agency resources: 8%
- Relies primarily on identity to allow access to agency resources: 20%

_BASE: 123_

Industry/Government Contractor Respondents
- Still relies heavily on perimeter defense tools / policies: 17%
- Is still evaluating tools to centrally manage identity / access to agency resources: 25%
- Has begun consolidation identity / access to agency resources: 25%
- Has mostly consolidation identity / access to agency resources: 17%
- Relies primarily on identity to allow access to agency resources: 17%

_BASE: 48_

My agency ...
- still relies heavily on perimeter defense tools / policies
- is still evaluating tools to centrally manage identity / access to agency resources
- has begun consolidation identity / access to agency resources
- has mostly consolidation identity / access to agency resources
- relies primarily on identity to allow access to agency resources

Q: How far along would you say your agency is in moving from a perimeter defense security approach to an identity-centered (zero-trust) approach?
(Select the most appropriate response)
Agencies’ efforts to meet federal identity management requirements

As federal agencies get up to speed on a larger approach to identity management, half of government respondents indicated their team has created a strategy to meet the requirements of OMB’s FICAM policy.

BEHIND THE FINDINGS:

On May 19, 2019 the White House’s Office of Management and Budget (OMB) released a memo outlining new objectives for securing federal IT systems, including a common vision for using identity and access management controls.

The policy sets deadlines for specific agencies to lead government-wide efforts to improve the management and use of digital identity such as the Department of Commerce, General Services Administration, Office of Personnel Management and the Department of Homeland Security.

Federal Government Respondents

Q: Have you or your team created a strategy to meet the requirements of the OMB Federal Identity, Credential and Access Management (FICAM) policy, published on May 19, 2019?

YES: 51%  
NO: 23%  
I DON’T KNOW: 26%

BASE: 123
Of government respondents whose agencies have a FICAM strategy, 49% reported their agency is on its way to consolidating — or relying primarily on — identity safeguards to control access to agency resources.

However, of those whose agencies do not have a FICAM strategy, only 36% are at a comparable stage.

Q: How far along would you say your agency is in moving from a perimeter defense security approach to an identity-centered (zero-trust) approach? (Select the most appropriate response)
How agencies perceive the importance of zero-trust strategies

The importance of zero trust:

To meet goals in improving citizen services
- 68% rate important to high priority

When expanding to the cloud
- 74% rate important to high important

As more apps and devices access agency resources
- 70% rate important to high priority

Q: How important is a zero-trust strategy to your agency’s ability:
- to achieve its goals in improving citizen services?
- to accommodate anticipated expansion into the cloud?
- to accommodate anticipated changes in the types of applications and devices used to access agency resources?
When agencies have a FICAM strategy, they prioritize zero-trust strategies more often.

Federal Government Respondents who have a FICAM strategy

To meet goals in improving citizen services

- 88%

- Federal Government Respondents who don’t have a FICAM strategy

- 38%

When expanding to the cloud

- 91%

- Federal Government Respondents who don’t have a FICAM strategy

- 47%

As more apps and devices access agency resources

- 90%

- Federal Government Respondents who don’t have a FICAM strategy

- 41%

Q: How important is a zero-trust strategy to your agency’s ability:
- to achieve its goals in improving citizen services?
- to accommodate anticipated expansion into the cloud?
- to accommodate anticipated changes in the types of applications and devices used to access agency resources?
Taking stock of who and what is on the network

The first step towards implementing a zero-trust strategy is to know who or what is accessing networks and applications. While a majority of government respondents said their agency has mostly or fully completed that task, between 41% and 48% said their agency is still in the early stages of that process.

Q: How far along is your agency in taking inventory of the following:

**People accessing agency systems**
- **BASE: 96**
  - **STARTED**: 17%
  - **IN PROCESS**: 31%
  - **MOSTLY COMPLETE**: 22%
  - **FULLY COMPLETE**: 26%

**Applications and other non-person entities**
- **BASE: 92**
  - **STARTED**: 15%
  - **IN PROCESS**: 30%
  - **MOSTLY COMPLETE**: 39%
  - **FULLY COMPLETE**: 15%

**Enterprise-owned devices**
- **BASE: 97**
  - **STARTED**: 15%
  - **IN PROCESS**: 26%
  - **MOSTLY COMPLETE**: 37%
  - **FULLY COMPLETE**: 22%

**Non-enterprise-owned devices**
- **BASE: 87**
  - **STARTED**: 14%
  - **IN PROCESS**: 31%
  - **MOSTLY COMPLETE**: 36%
  - **FULLY COMPLETE**: 20%

**Business processes involving identity and access**
- **BASE: 93**
  - **STARTED**: 15%
  - **IN PROCESS**: 33%
  - **MOSTLY COMPLETE**: 26%
  - **FULLY COMPLETE**: 26%

*Excludes those who selected “I don’t know”

BEHIND THE FINDINGS:

The Federal Government’s Continuous Diagnostics and Mitigation (CDM) program requires agencies to identify “who” and “what” is on their networks.

However, limited funding for CDM continues to restrain efforts to leverage identity to refresh applications and adopt cloud services, according to agency executives.
Setting the foundational blocks for zero-trust architecture

Establishing a zero-trust environment requires a combination of capabilities. Nearly half or more of respondents said their agency/organization had minimal to average capabilities in determining which devices are owned by the enterprise and which are not; or whether communications and individual connections are secure.

<table>
<thead>
<tr>
<th>MINIMALLY CAPABLE</th>
<th>HIGHLY CAPABLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>We are able to determine which systems and devices are owned or managed by the enterprise and which are not.</td>
<td></td>
</tr>
<tr>
<td>13%</td>
<td>20%</td>
</tr>
<tr>
<td>All communication to agency resources is secure regardless of whether it’s from inside or outside the network perimeter.</td>
<td></td>
</tr>
<tr>
<td>8%</td>
<td>30%</td>
</tr>
<tr>
<td>Access to individual enterprise resources is granted on a per-connection basis.</td>
<td></td>
</tr>
<tr>
<td>9%</td>
<td>23%</td>
</tr>
</tbody>
</table>

Q: How would you rate your agency’s current capability to ensure the following security measures? (On a scale of 5 to 1: where 5 is highly capable – best in class standards – and 1 is minimally capable)
Setting the foundational blocks for zero-trust architecture

Similarly, almost half of respondents said their agency/organization had minimal to average capabilities to control access to resources based on user behavior, or dynamically enforce user authentication before access is allowed.

Access to resources is determined by policy and observable user behavioral attributes.

Enterprise systems are in their most secure state (e.g. patches are current).

User authentication is dynamic and strictly enforced before access is allowed.

Q: How would you rate your agency's current capability to ensure the following security measures? (On a scale of 5 to 1: where 5 is highly capable – best in class standards – and 1 is minimally capable)

BASE: 171
IT leaders see user authentication capabilities as important for better security. However, there are a range of solutions to get there.

Respondents ranked **multi-factor one-time password (33%)**, **randomly chosen password/PIN (22%)** and **out-of-band authenticators (20%)** as the top three types of MFA their agencies will increase investment over the next two years.

**Q:** What kind of alternative or multi-factor authentication will your agency invest more in over the next 2 years?
(Select all that apply)

*Excludes “I don’t know” – 28%, and “Other” (PIV and CAC cards) – 2%*
Plans to implement a password-less user experience

Respondents indicated their organizations are moving towards a password-less user experience with a little more than half planning to do so within the next 2 years.

Q: Is your agency planning to implement a password-less user experience...?

BEHIND THE FINDINGS:
"A new standard known as Web Authentication, or WebAuthn for short, is a credential management API that will be built directly into popular web browsers. It allows users to register and authenticate with web applications using an authenticator such as a phone, hardware security keys or trusted platform module (TPM) devices."
– Nick Steele, Duo Security
Respondents ranked a lack of staff expertise as a greater obstacle over budget limitations to adopting zero-trust practices. But they also cited a lack of standardized capabilities and agency policies and widespread IT independencies as key challenges.

All Respondents

1. **42%** - Lack of staff expertise
2. **36%** - Insufficient budget
3. **30%** - A lack of standardized IT capabilities
4. **30%** - Widespread interdependencies within or across agencies
5. **30%** - A lack of agency policies and processes
6. **20%** - Acquisition challenges to procure zero-trust enabling technology
7. **17%** - Inadequate network visibility

*Excludes “Other,” (i.e. poor management, culture, unknown) - 8%  BASE: 171

**Q:** What challenges are keeping your agency from adopting a zero-trust strategy? (Select up to three)

**Q:** Does your agency currently have the ability to automatically provision and deprovision access rights for users as they join, move within or leave the organization?

**AUTOMATIC PROVISIONING**

Just over half of federal government respondents report their agency can automatically provision and deprovision access rights for users as they join, move within or leave the organization.

**Federal Government Respondents**

- **58%** - YES
- **20%** - NO
- **22%** - I DON'T KNOW

BASE: 123

fed scoop
Federal Identity, Credential and Access Management (FICAM) as a means for securing federal resources has become increasingly essential for the federal government to successfully deliver its promises and services to the American public.

The findings in this report make it plain that agencies with comprehensive FICAM and zero-trust strategies are better positioned to:

- Improve their risk management and security posture.
- Expand more readily to multi- and hybrid cloud environments.
- Accommodate the rapid evolution of applications and devices accessing agency resources.
- Deliver superior user experiences for the public and federal employees.

The findings also point to accelerating interest in moving toward a password-less user experience — and increased investments in multifactor approaches including one-time password, randomly chosen password / PIN, and out-of-band over the next two years.

While the standards for creating a Zero Trust Architecture ecosystem are still evolving, agencies now have access to valuable resources to guide their efforts, including:

- NIST’s draft publication on Zero Trust Architecture components and NIST’s “Digital Identity Guidelines” publication series.
- GSA’s guide to Identity Management and catalog of ICAM solutions and shared services.
**FedScoop** is the leading tech media brand in the federal government market. With more than 210,000 unique monthly visitors and 120,000 daily newsletter subscribers, FedScoop gathers top leaders from the White House, federal agencies, academia and the tech industry to discuss ways technology can improve government and identify.

**CONTACT**

**Wyatt Kash**  
Senior Vice President Content Strategy  
Scoop News Group, Washington, D.C.  
202.887.8001  
wyatt.kash@scoopnewsgroup.com