NASTD
National Association of State Technology Directors

JANUARY 2024

State Government's Identity and Access Management Strategy: Plans and Progress

Introduction

Organizations in both the public and private sectors use identity and access management (IAM) strategies and solutions to ensure secure access and management of sensitive information. These approaches streamline and centralize the management of identities, access and permissions across the organization. State government central information technology authorities can reduce the risk of data breaches while efficiently managing systems, applications and data while complying with security and privacy regulations.

In 2023, the National Association of State Technology Directors' (NASTD) Executive Board charged its Research Committee with surveying its state members on the status of state identity access and management efforts.

Methodology

NASTD, with the assistance of the National Association of State Chief Information Officers (NASCIO), distributed an Internet survey to all 50 state central IT authorities in July 2023. Thirty-two states submitted responses to the survey: Alabama, Arizona, Arkansas, California, Connecticut, Delaware, Georgia, Illinois, Kentucky, Louisiana, Maine, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, New Hampshire, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Vermont, Washington, West Virginia, Wisconsin and Wyoming.

NASTD's Research Committee, comprised of state government information technology members and association staff, developed the survey questions.

NASTD Contact:
Rick Woodruff
NASTD President
Phone: (502) 782-3795
rick.woodruff@ky.gov

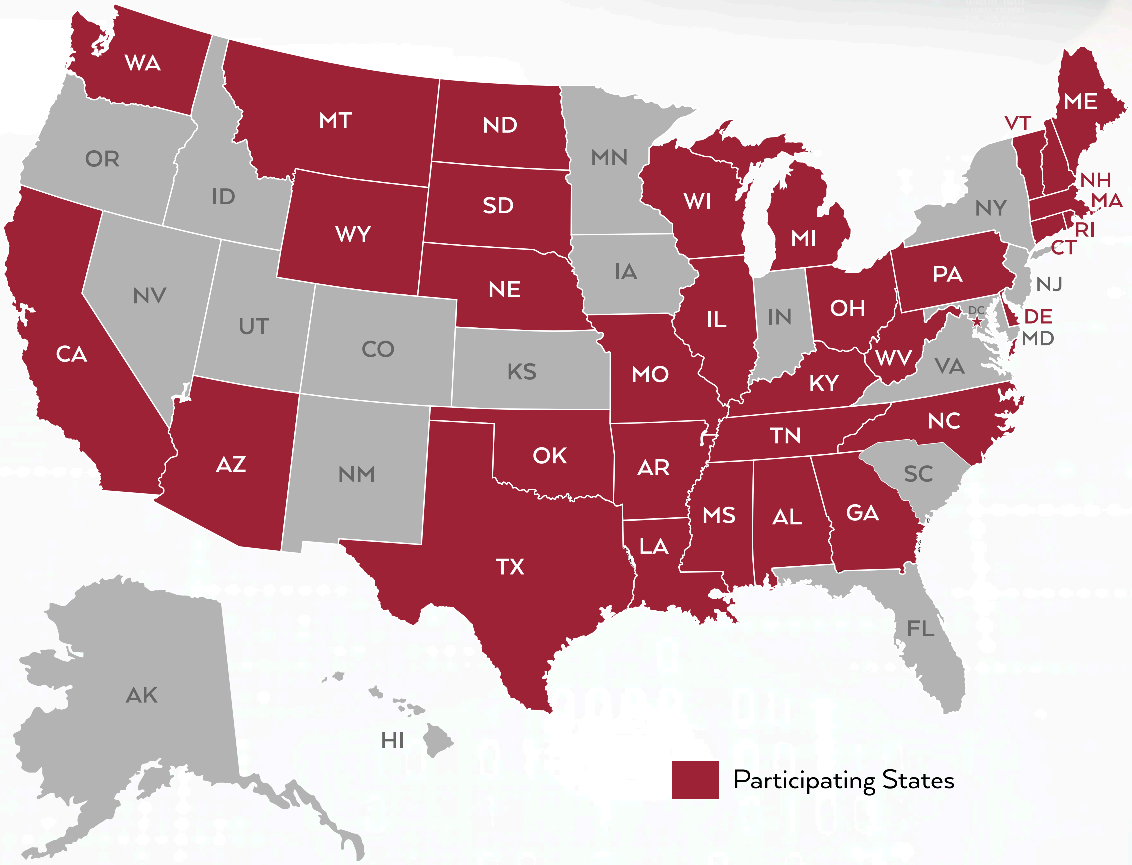
NASTD is a dynamic, member-driven association committed to advancing the effective use of information technology to achieve operational efficiency in state government.

For more information, visit ***www.nastd.org***

1776 Avenue of the States
Lexington, KY 40511-8482
Phone: (502) 244-8000
nastd@csg.org

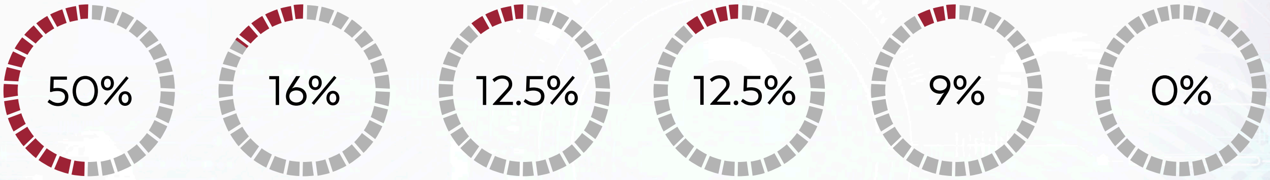
NASTD

National Association of State Technology Directors



Survey Results

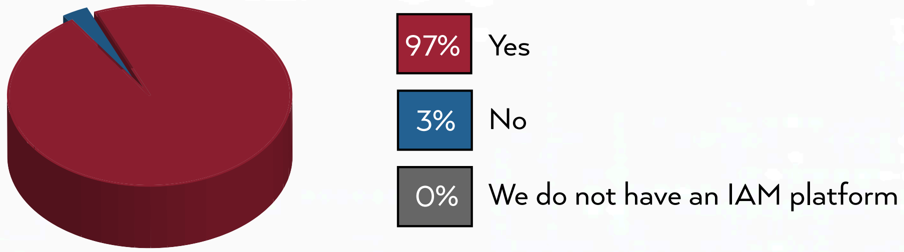
What is the scope of your state's identity and access management (IAM) strategy?



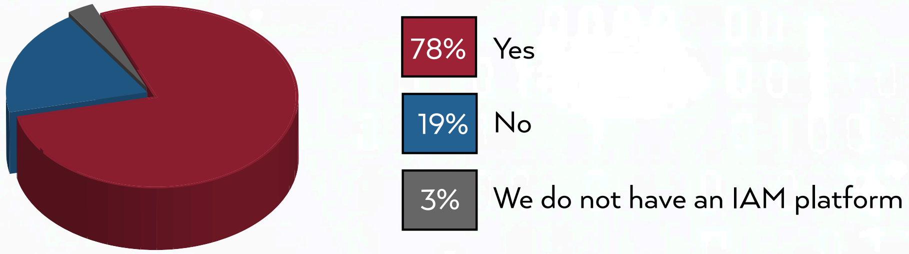
50%	16%	12.5%	12.5%	9%	0%
Focus on employees, citizens/residents, vendors/contractors and businesses	Focus on employees and citizens/residents	Focus on employees, citizens/residents, and vendors/contractors	Focus on employees and vendors/contractors	Focus on employees	We do not have an IAM strategy/policy

National Association of State Technology Directors

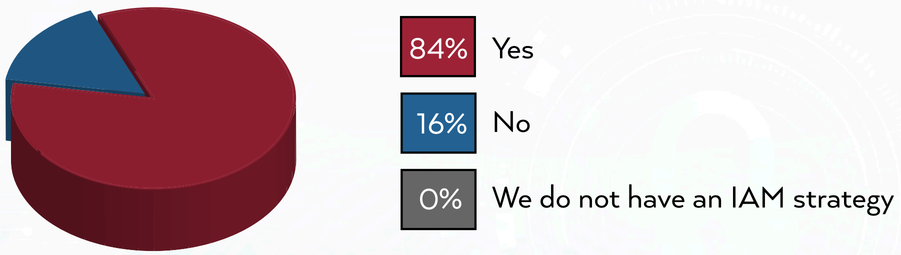
Does your IAM platform integrate with Active Directory, Azure Active Directory, etc.?



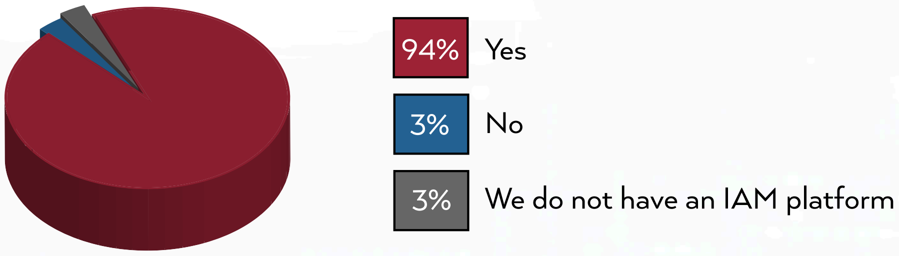
Does your IAM platform support policy-driven verification?



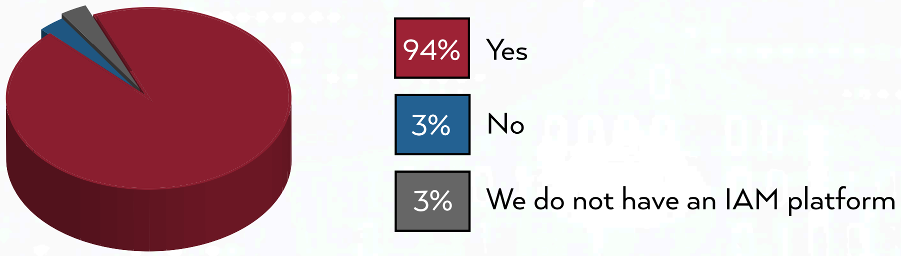
Does your IAM strategy require multi-factor authentication?



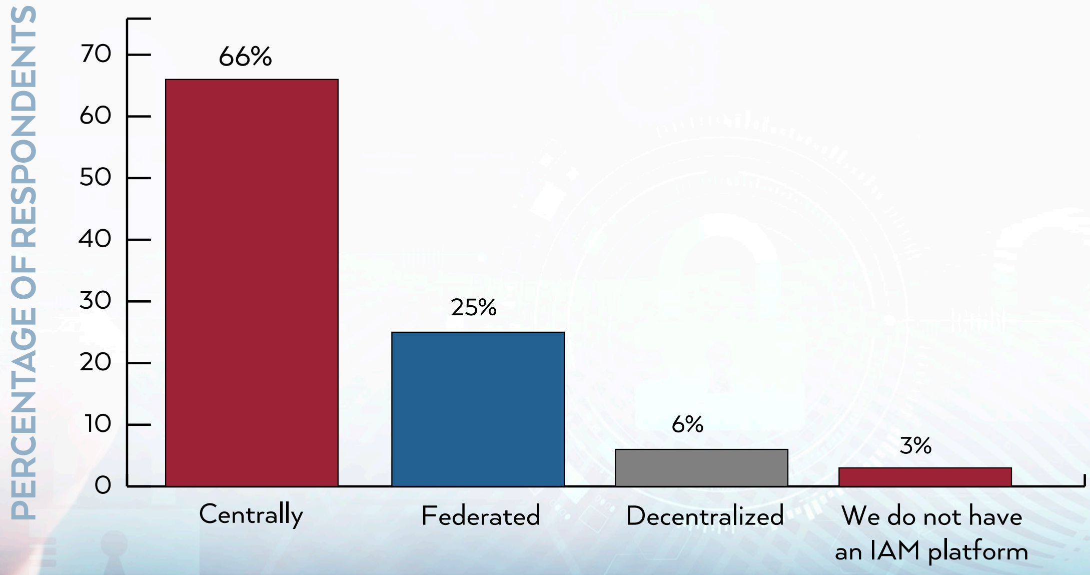
Does your IAM platform support federated sign-on?



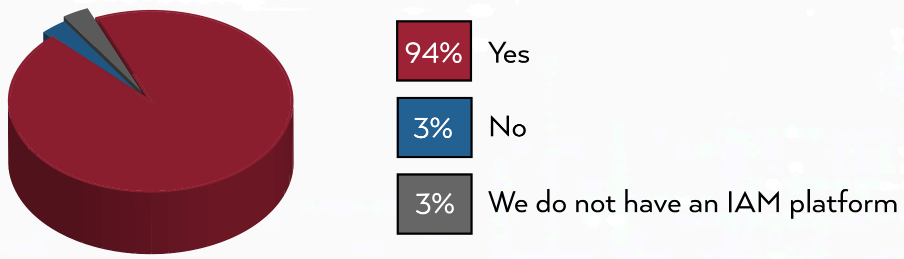
Does your IAM platform allow for self-service password changes for users?



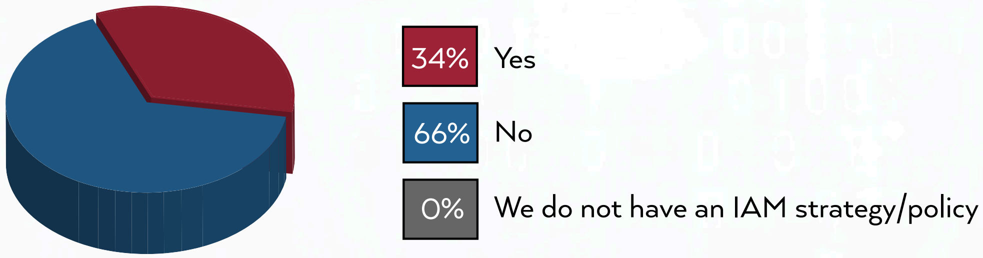
Is your IAM platform administered centrally, federated or decentralized?



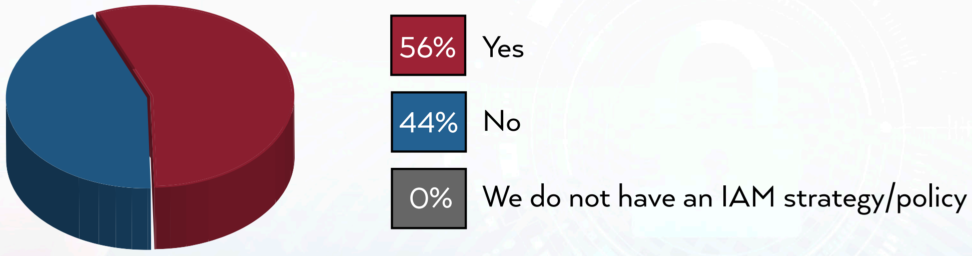
Does your IAM platform support a robust list of automated connectors (API, SAML 2.0, OpenID, oAuth, AAA, etc.)?



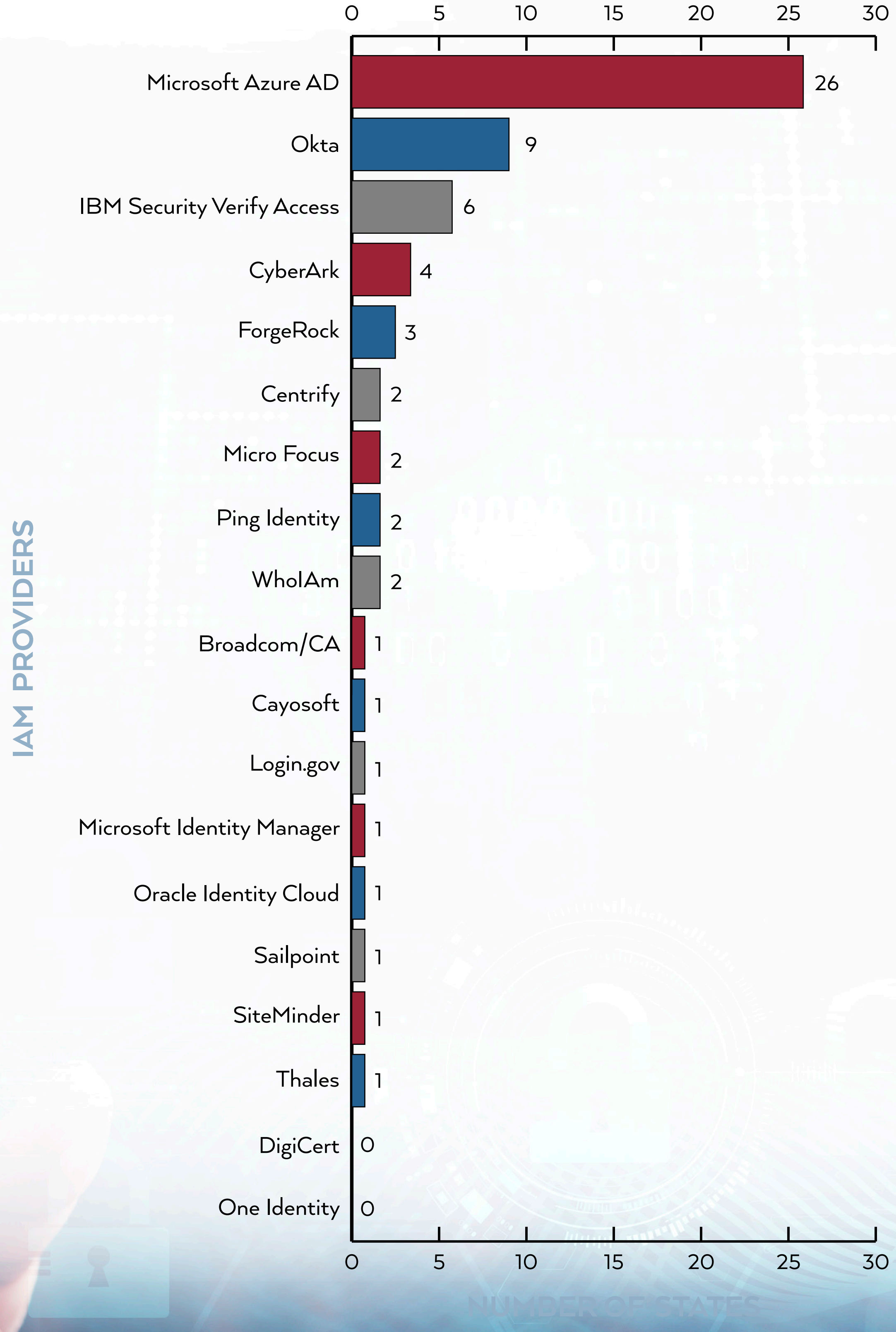
Does your IAM strategy support any physical components such as ID badges, smart cards or RFID?



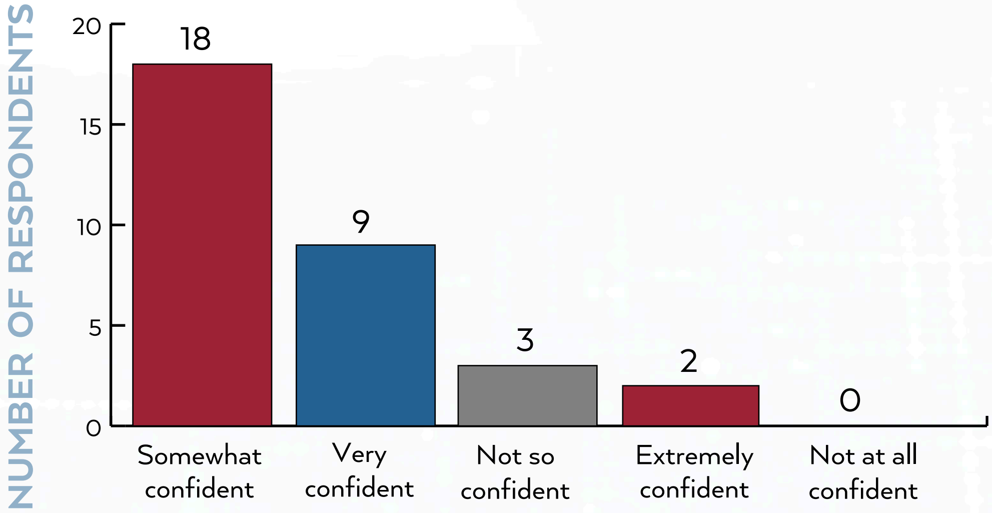
Does your IAM strategy involve supporting more than one identity provider?



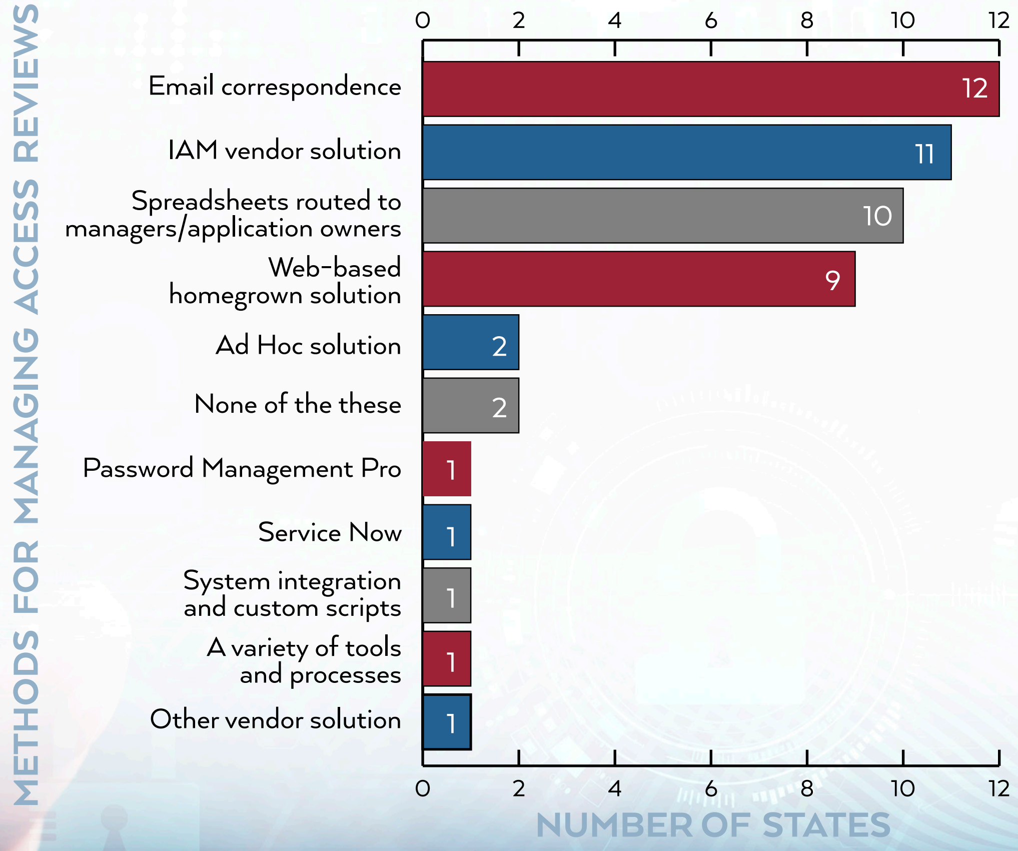
Please identify which IAM provider(s) you utilize? (Select all that apply.)



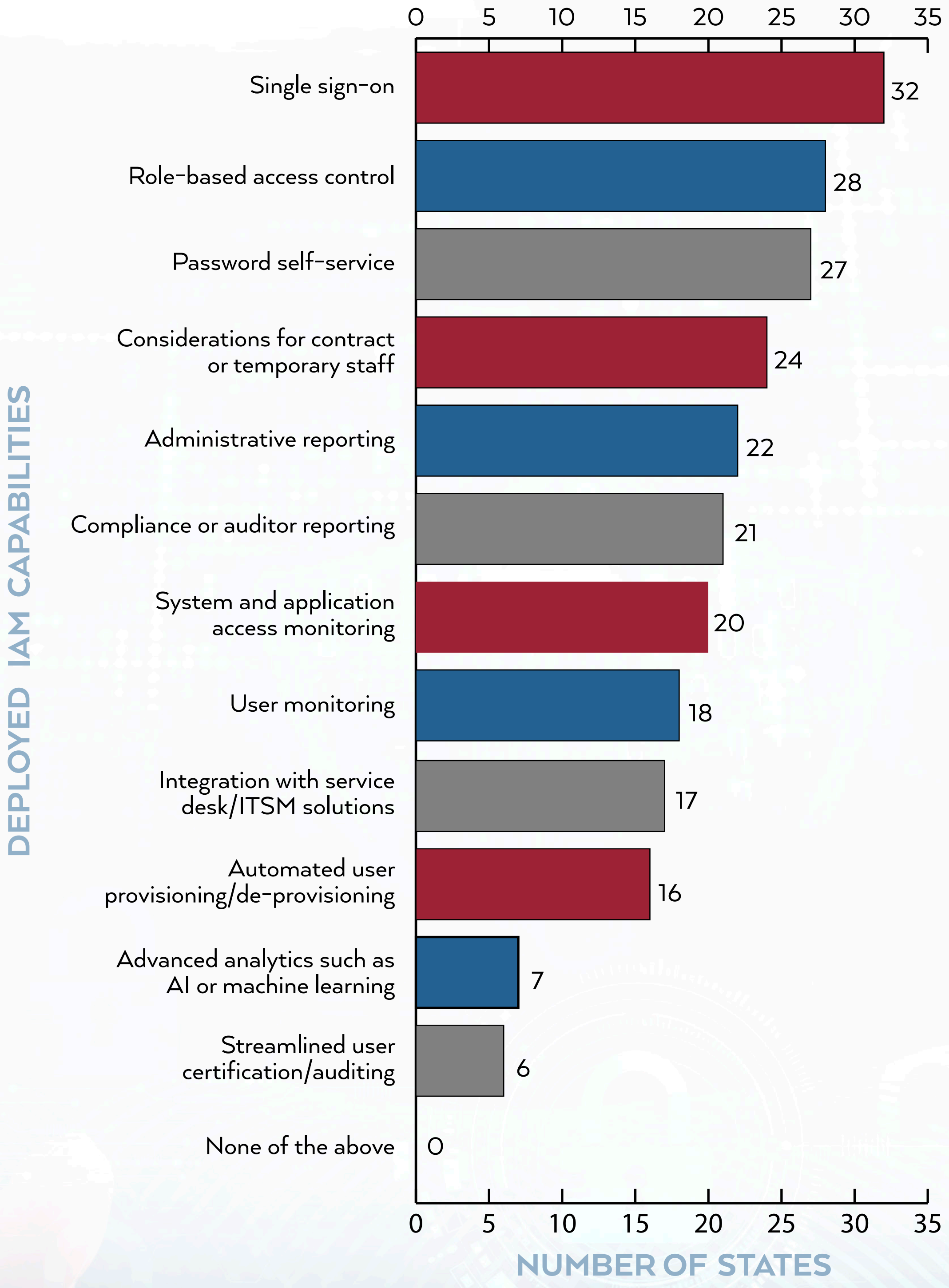
How confident are you in your organization's privilege access management?



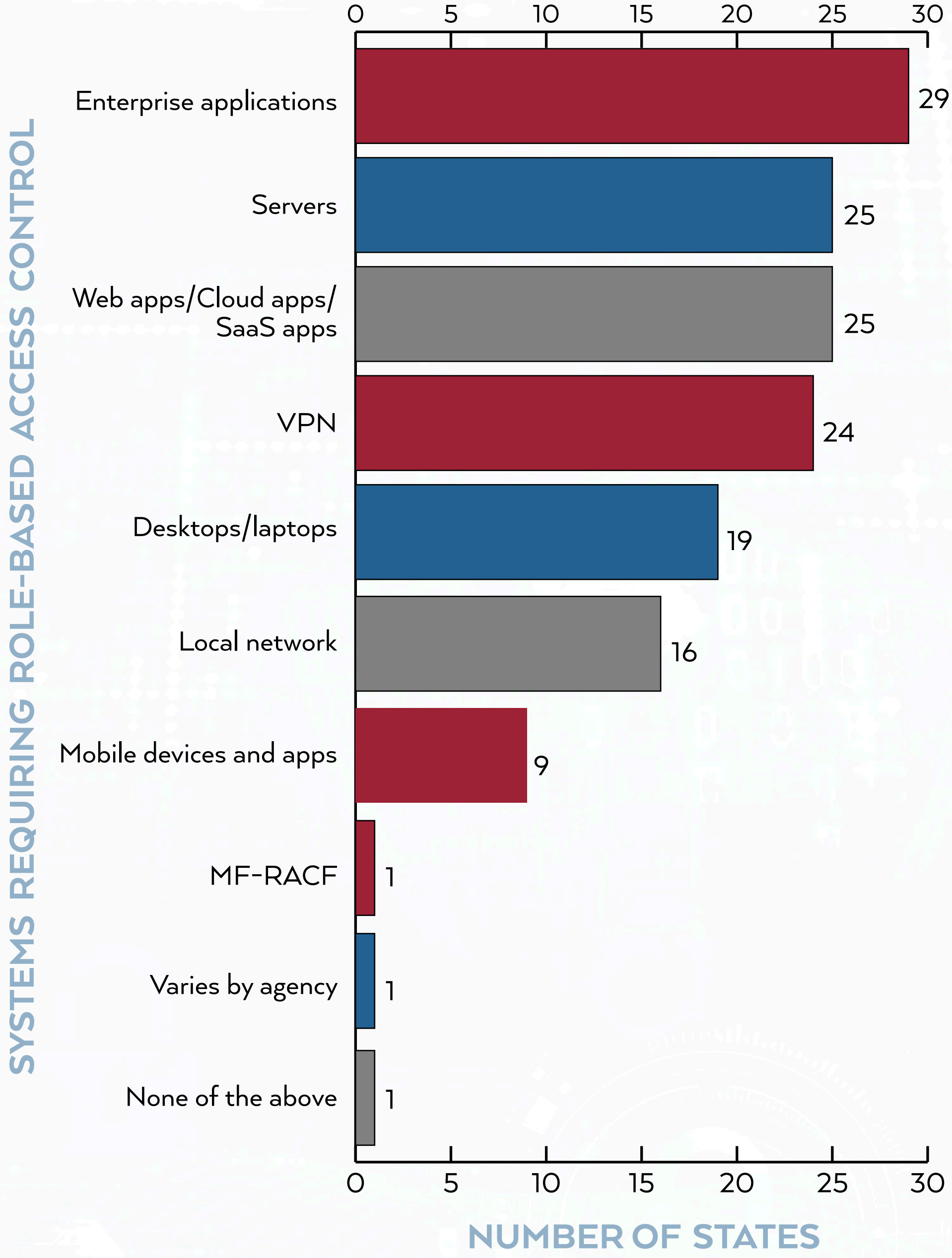
What methods do you utilize for managing access reviews? (Select all that apply.)



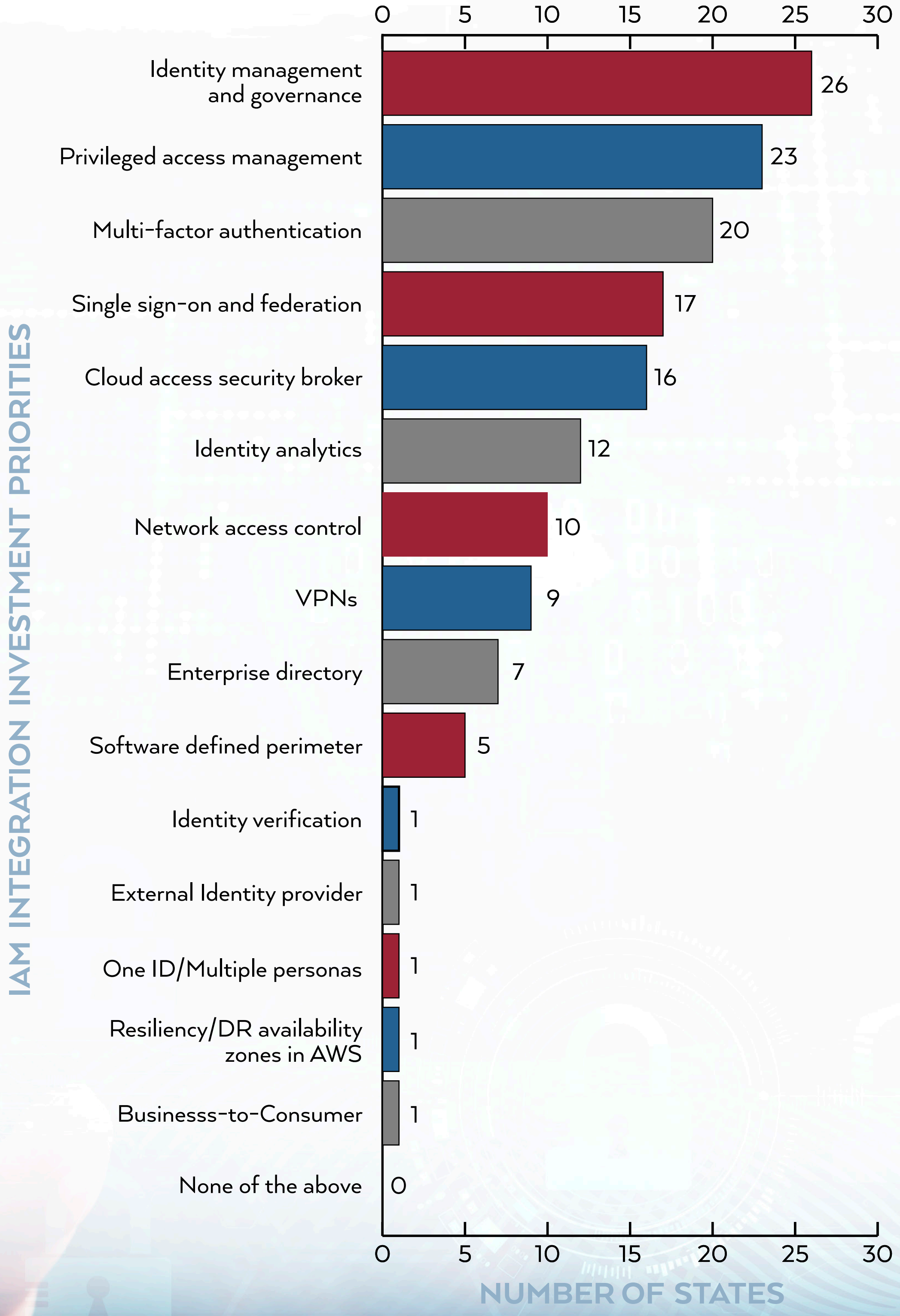
What IAM capabilities are deployed in your state? (Select all that apply.)



Which systems in your state require role-based access control? (Select all that apply.)

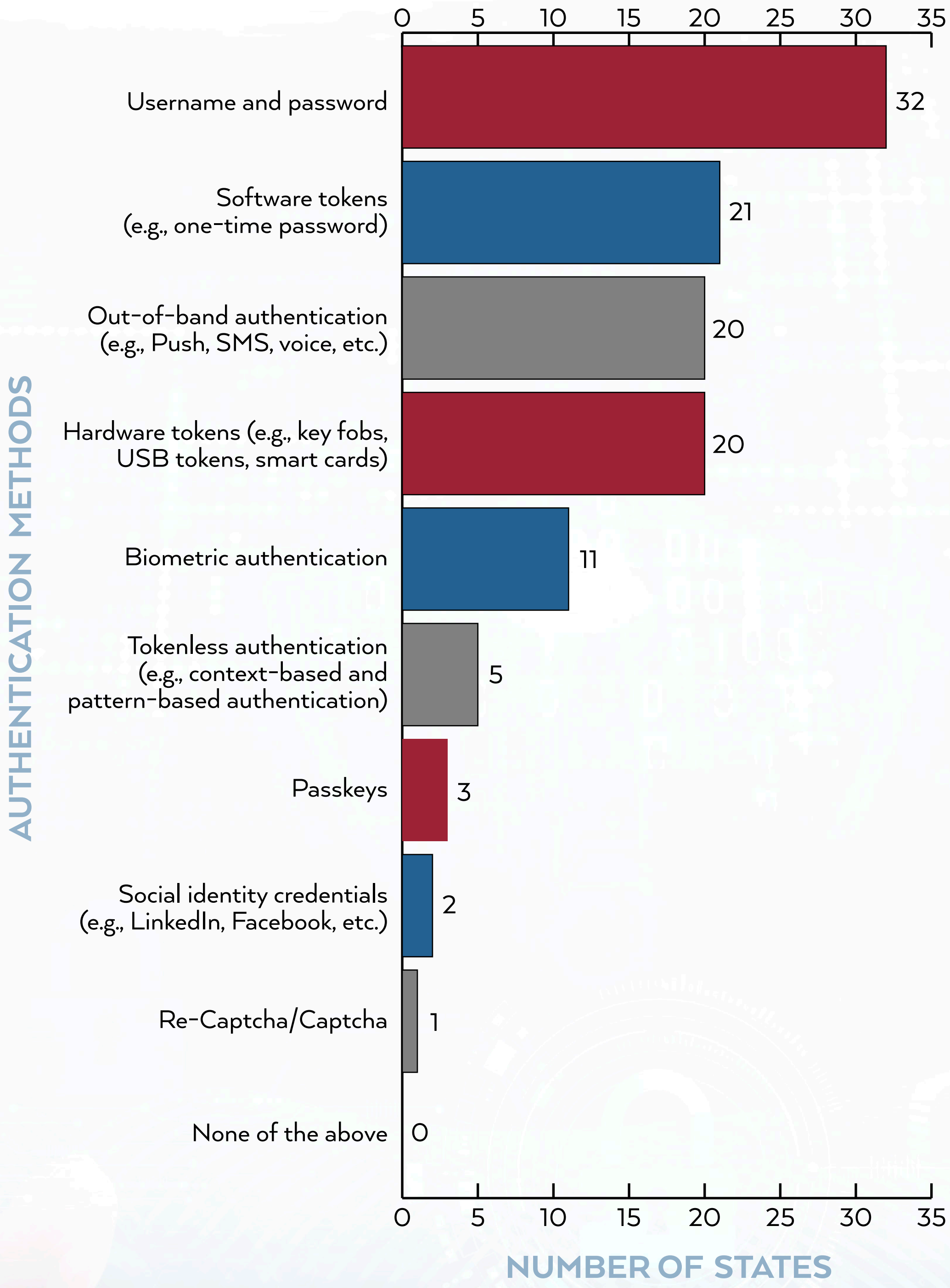


Which of the following areas are a priority for investment of IAM integration in your state for the next planning cycle? (Select all that apply.)

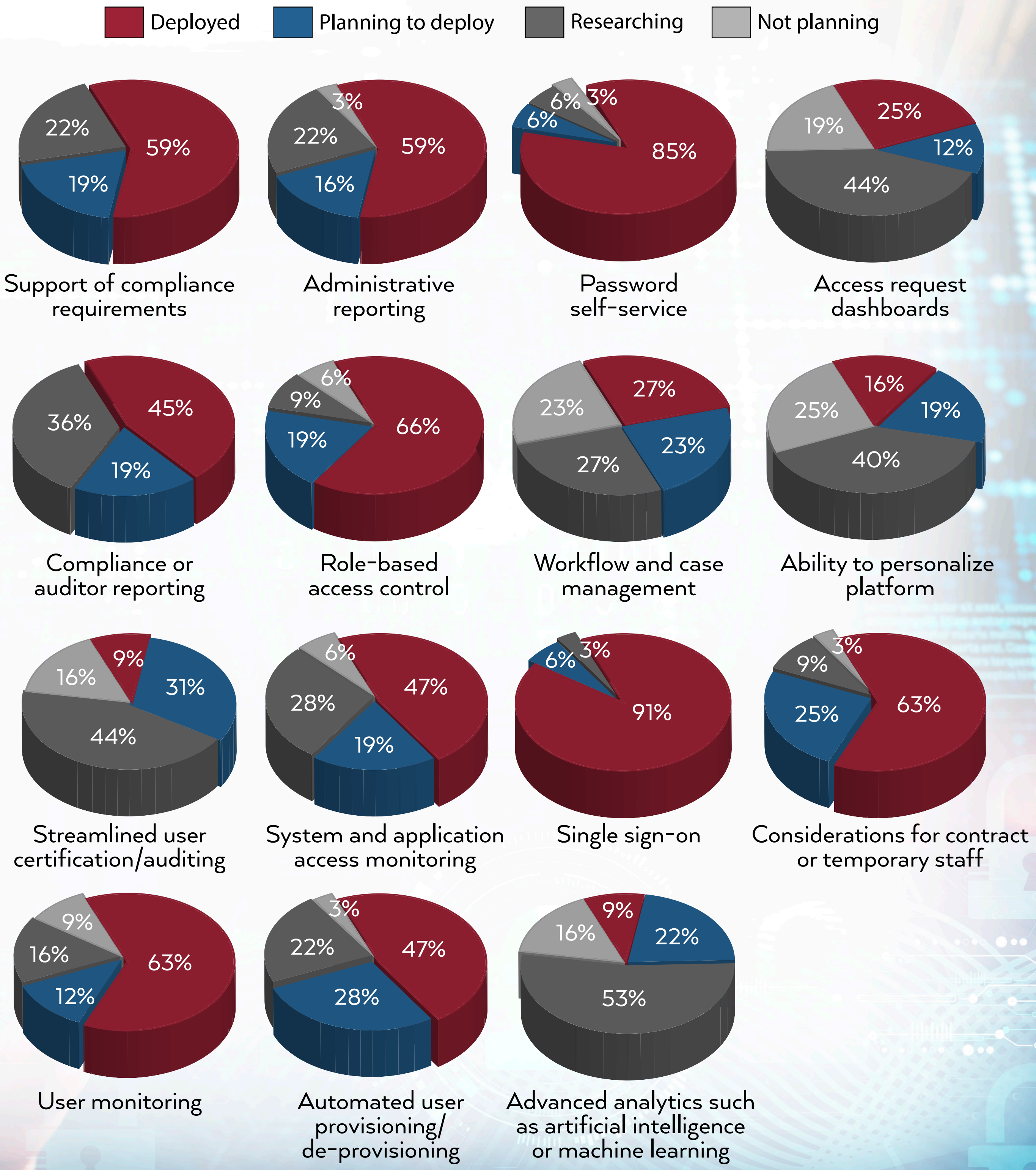


National Association of State Technology Directors

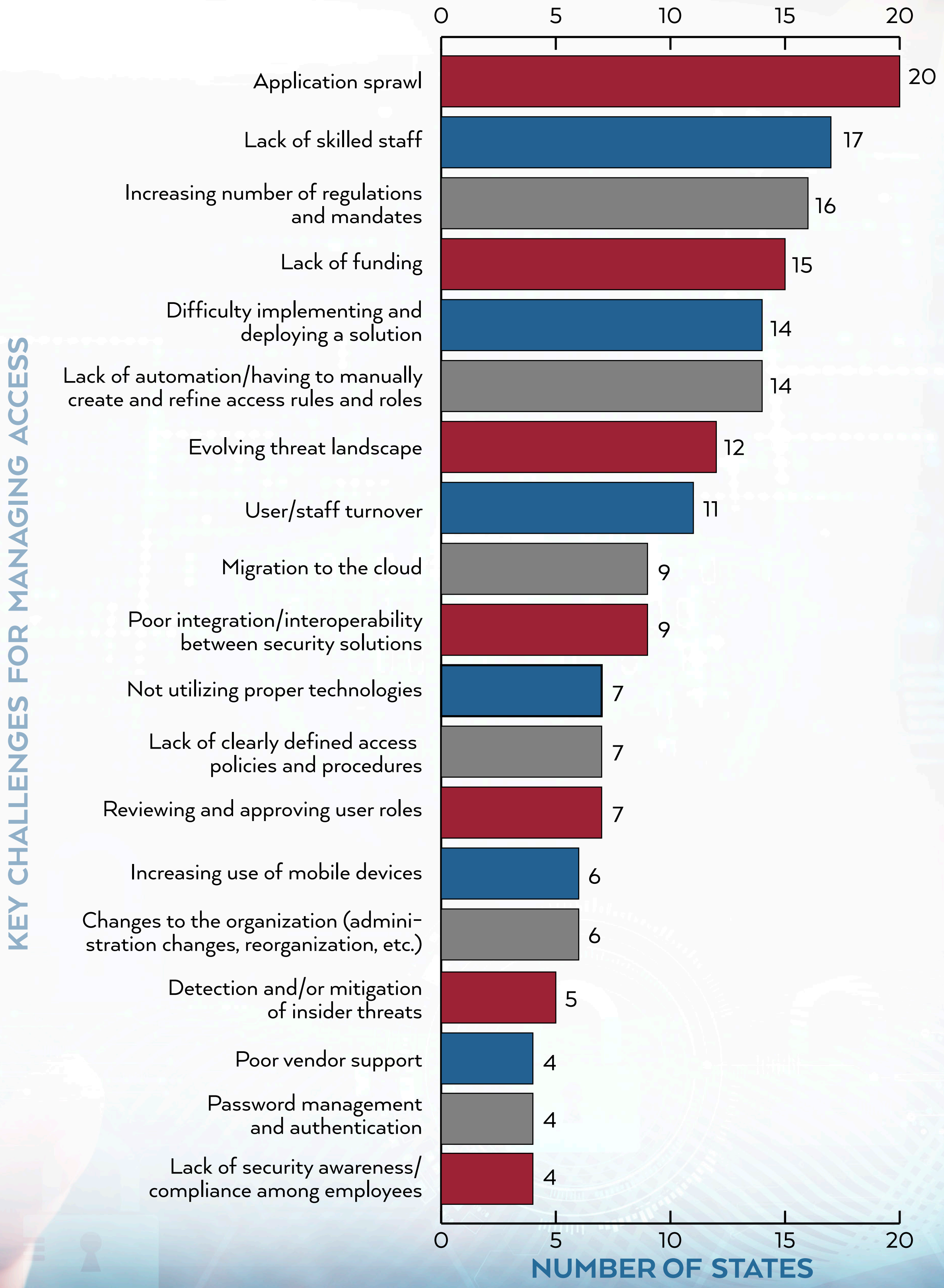
What authentication methods are used in your state? (Select all that apply.)



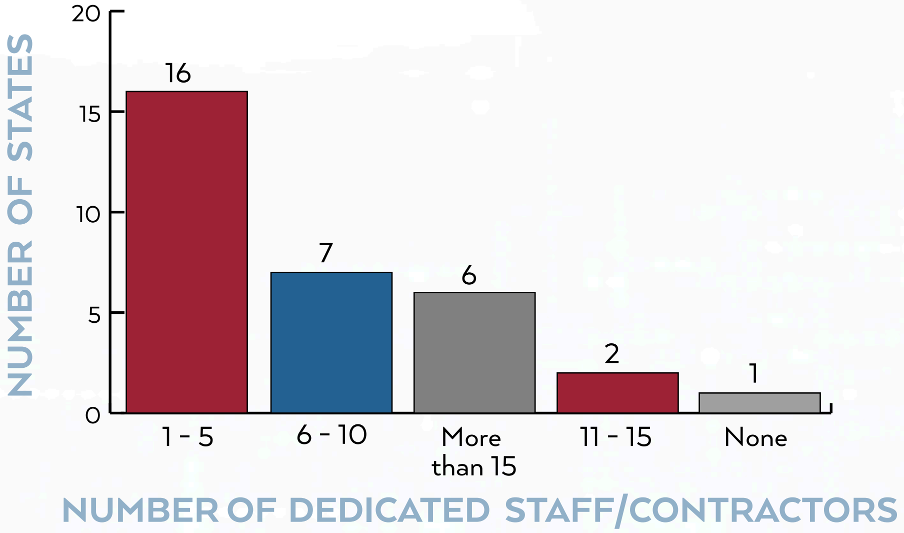
How has your state prioritized the following IAM capabilities?



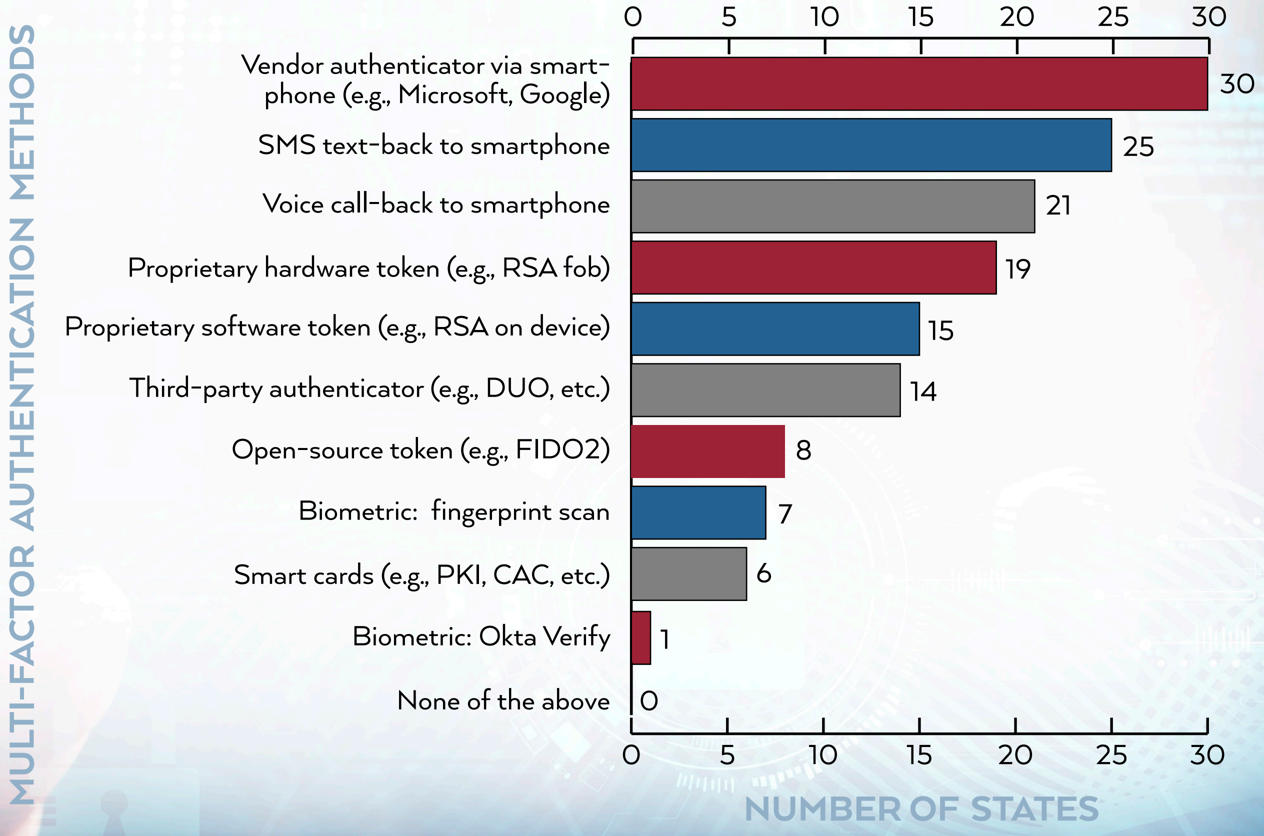
What are the key challenges for managing access in your state? (Select all that apply.)



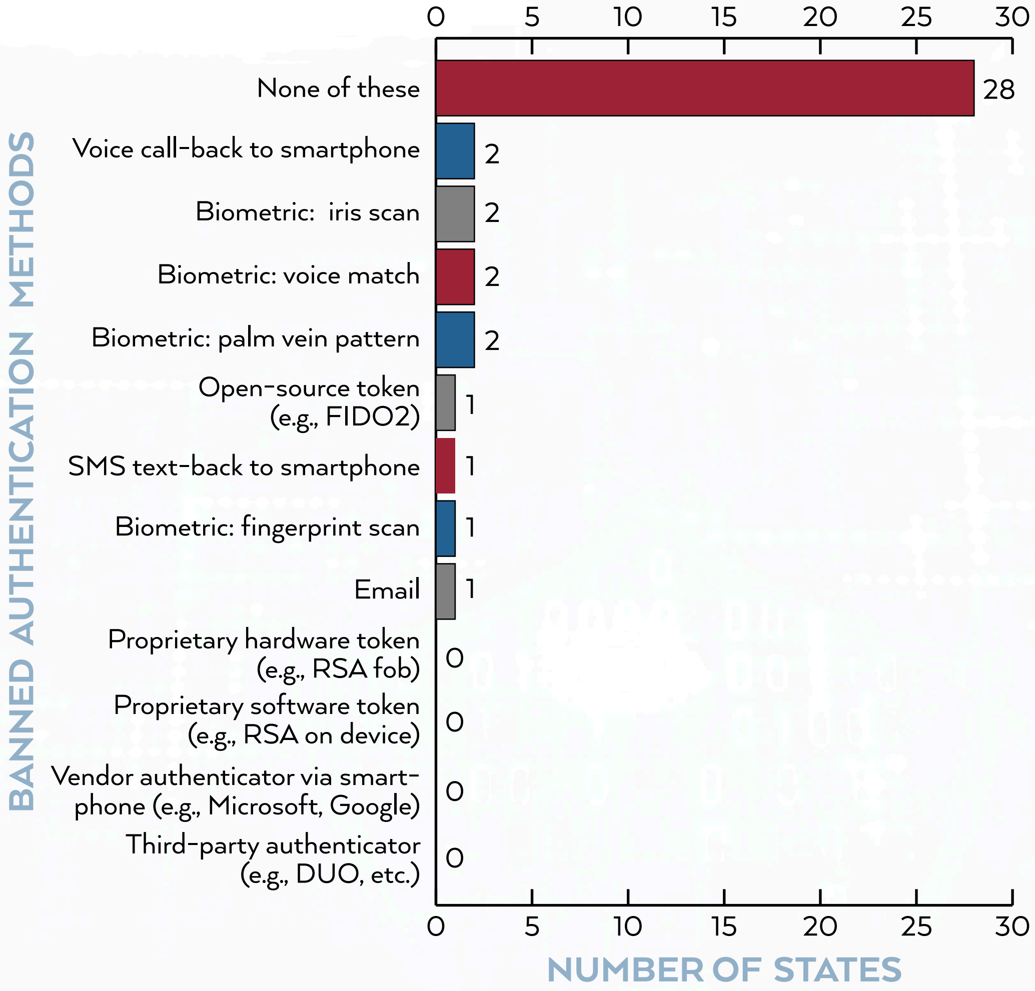
How many staff/contractors do you have dedicated to IAM?



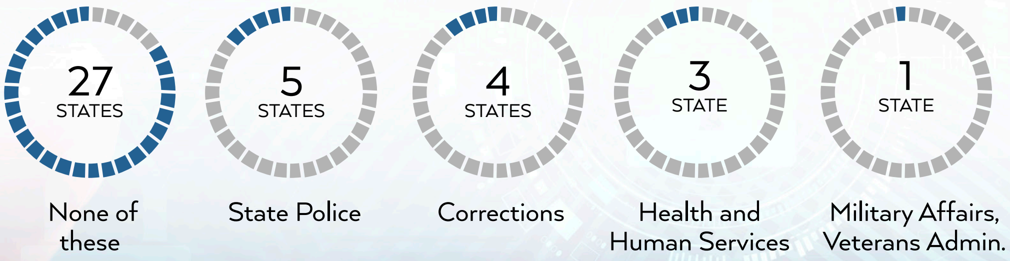
Which multi-factor authentication methods does your IAM solution support? (Select all that apply.)



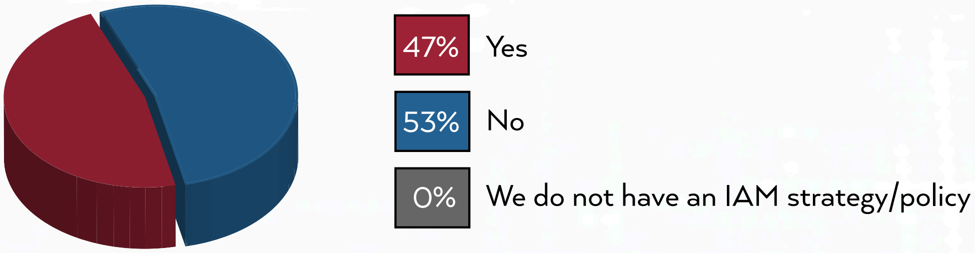
What authentication methods are banned in your state? (Select all that apply.)



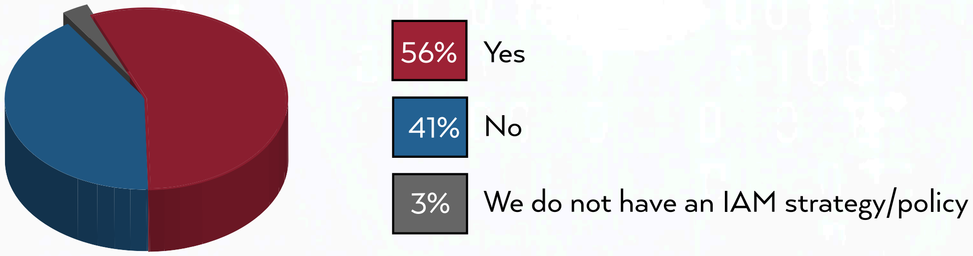
If any authentication methods are banned, which agencies have more stringent requirements? (Select all that apply.)



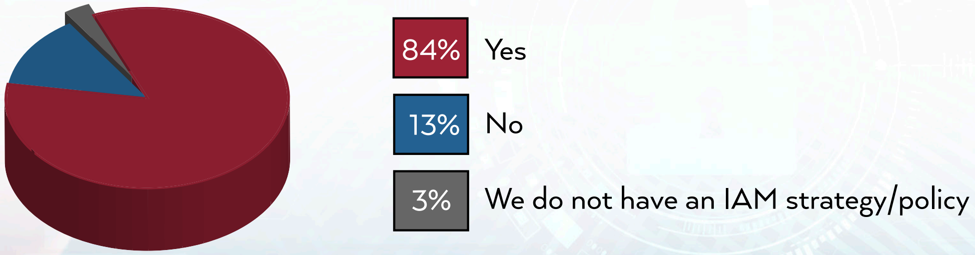
Does your IAM policy require a separate device to authenticate for NIST moderate and NIST high data classifications?



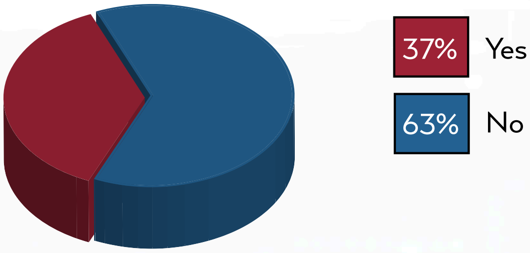
Does your IAM and body of policy allow the use of non-proprietary authentication devices (e.g., FIDO2/FIDO Alliance keys, YubiKeys, third party-authenicators, etc.)



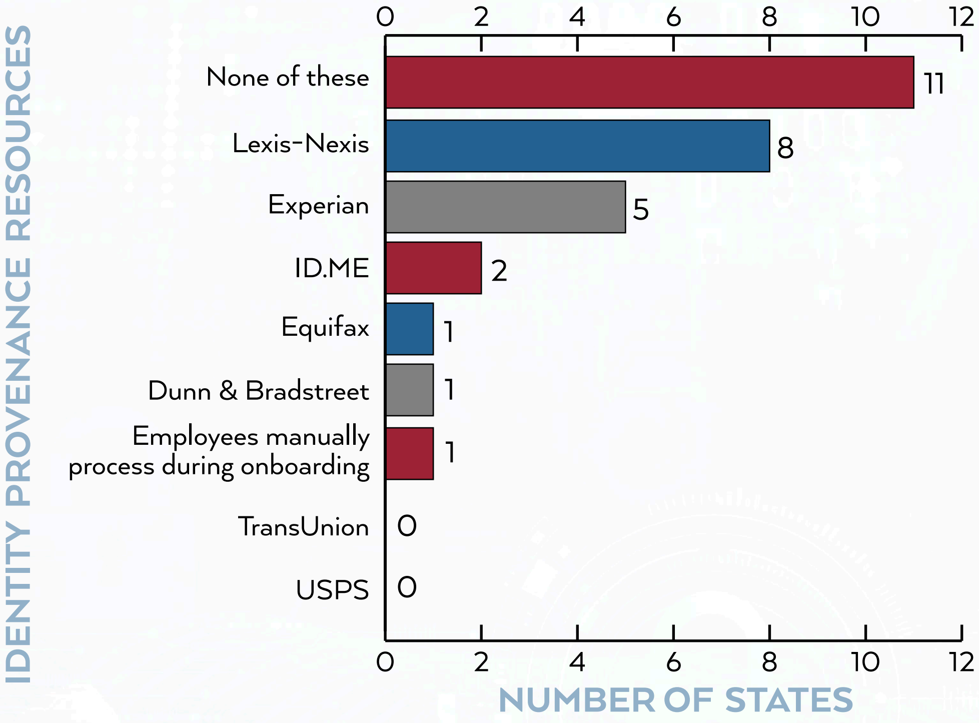
Does your IAM solution support geo-fencing?



Does your state use an identity provenance resource to validate prospective users?



If you answered "yes" to the previous question, which apply? (Select all that apply.)



Summary

Half of state respondents have a comprehensive strategy in place for IAM focusing on employees, citizens/residents, vendors/contractors and businesses. Three states are focusing on employees only with the remaining 13 states somewhere in between.

An overwhelming majority of 31 state respondents indicated their IAM platform integrates with Active Directory and/or Azure Active Directory. Only one state does not currently have any IAM platform in place.

Some of the other IAM facts from our survey:

- 94% of IAM platforms support federated sign-on and allow for user self-service password changes.
- 84% require multi-factor authentication.
- 78% of respondent IAM platforms support policy-driven verification.

Concerning how responding states administer their IAM platforms: 21 states administer them centrally, eight follow a federated model and two states follow a decentralized model.

Another overwhelming majority of state respondents (94%) support automated connectors such as API, SAML 2.0, OpenID, oAuth and AAA.

Approximately one-third of survey respondents (34%) support physical components such as identification badges, smart cards or RFID while 66% do not support such components.

There is a slight difference in IAM strategies utilizing more than one identity provider with 56% of respondents using more than one and 44% using one. State respondents preferred IAM providers in use are Microsoft Azure AD (81%), Okta (28%), IBM Security Verify Access (19%) and CyberArk (12%). Other solutions providers totaled less than ten percent.

Our research committee found it significant that most state respondents see the need for improvement in their privilege access management (PAM) practices, with 21 states somewhat confident or not so confident in their practices. Two states were extremely confident and nine very confident in their PAM practices.

Respondents utilize a balanced portfolio of methods for managing access reviews, including: email correspondence (38%), IAM vendor solutions (34%), spreadsheets routed to managers or application owners (31%) and homegrown web-based solutions (28%). One respondent said, "Agencies use a variety of tools and processes depending on their maturity levels with their processes."

The topmost IAM capabilities deployed by state respondents are: single sign-on (100%), role-based access control (87%), password self-service (84%), considerations for contract or temporary staff (75%),

administrative reporting (69%) and compliance or auditor reporting (66%). These findings indicate states are thinking security first while also keeping ease of use and management in mind.

The top state systems that require role-based access control are: enterprise applications (91%), servers (78%), web apps/cloud apps/software as a service apps (78%), virtual private network (75%) and desktops/laptops (59%).

State respondents identified the following areas as top priorities for investment in their next planning cycle: identity management and governance (81%), privileged access management (72%), multi-factor authentication (63%), single sign-on and federation (53%) and use of a cloud access security broker (50%).

More than 75% of state respondents are deploying or planning to deploy: single sign-on (97%), password self-service (91%), considerations for contract or temporary staff (88%), role-based access control (85%) and support of compliance requirements (78%).

All state respondents are using usernames and passwords as authentication methods. The next three favorite methods are: software tokens (66%), hardware tokens (63%), and out-of-band authentication (63%).

The biggest challenges state respondents indicated for managing access in their states were: application sprawl (63%), lack of skilled staff (53%) and an increasing number of regulations and mandates (50%).

Half of state respondents dedicate one to five staff members and/or contractors to IAM. Six states are utilizing more than 15 staff. There was not a direct correlation between the size of the state and the number of staff dedicated to IAM efforts.

The top state IAM solutions supporting multi-factor authentication methods are: vendor authentication via smartphone (94%), SMS text-back to smartphone (78%), voice call back to smartphone (66%) and the use of a proprietary hardware token (59%).

A significant majority of state respondents (88%) do not ban the use of any authentication methods with only a handful of states banning methods such as biometrics and more commonly employed methods such as SMS and voice calls back to a smartphone. State agencies that do ban these methods are state police, corrections departments, health and human services or military affairs/veterans administrations.

Fifteen state respondents require a separate device to authenticate for NIST moderate and NIST high data classifications. Seventeen states do not require a separate device.

A narrow majority of state respondents (56%) allow the use of non-proprietary authentication devices such as FIDO2/FIDO alliance keys, YubiKeys, or third-party authenticators.

In other findings, 84% of state respondents support geo-fencing in their IAM solutions. Twelve state respondents use an identity provenance resource to validate prospective users, using solutions from Experian, Equifax, Lexis-Nexis, Dunn & Bradstreet or ID.me. Again, security is a high priority for the states.

Outlook

State government IAM strategies continue to evolve. One respondent summarized it as follows, "Identity is ever evolving, and we are doing everything we can to keep pace. Security is priority one in all we tackle."

"This is an important initiative which requires significant planning and effort," said another state respondent. Another respondent added, "We've made great strides in the past few years to modernize and professionalize IAM, but still have much integration to do."

States are incorporating IAM efforts into their strategic IT plans, building out their strategies with supporting technologies, projects and objectives. One respondent noted, "It is certainly an area we expect to invest more in, mature and be part of all our device and application management efforts going forward."

State central IT authorities, sharing information with other states and partnering with private sector solutions providers, will leverage the NASTD community in these ongoing efforts.

About NASTD

The National Association of State Technology Directors - Technology Professionals Serving State Government, is a member-driven organization whose purpose is to advance and promote the effective use of information technology and services to improve the operation of state government.

State members provide and manage state government technology services and facilities for state agencies and other public entities, often including hospitals, prisons, colleges and universities. These members also play a strategic role in planning and shaping state government information technology infrastructures and policies. Corporate members provide information technology services and equipment to state government.

NASTD was founded in 1978 and has been an affiliate of The Council of State Governments (CSG) since 1980. For more information about NASTD, visit *www.nastd.org*.

Acknowledgements

Along with the NASTD state members who submitted responses to the survey, NASTD thanks the following for their contributions:

- Bob Campbell, Chief Technology Officer, state of Tennessee
- Paul Czarnecki, Communications and Research Manager, National Association of State Technology Directors
- Paul Groll, Director, Emerging Technology Research & Architect, state of Michigan
- Kim McBride, Owner/Graphic Designer, McBride Design
- Mark McCord, Executive Director, National Association of State Technology Directors
- Andy Ogan, Tele Enterprise Architecture Manager, state of South Dakota
- Dawnna Pease, Director Computing Infrastructure and Services, state of Maine, committee chair
- Doug Robinson, Executive Director, National Association of State Chief Information Officers
- Cindy Smith, Deputy Chief Information Officer, state of West Virginia
- Meredith Ward, Deputy Executive Director, National Association of State Chief Information Officers