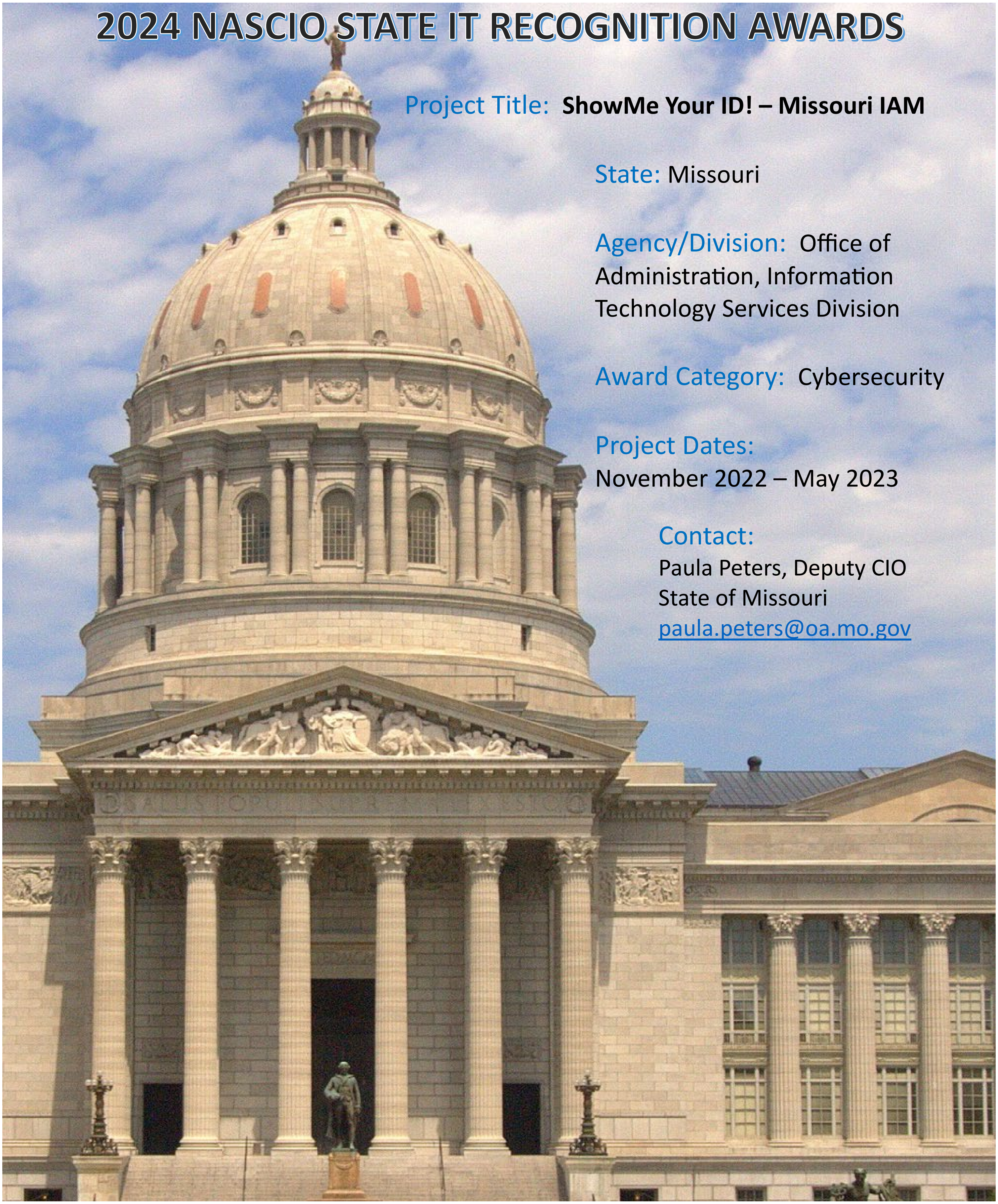
2024 NASCIO STATE IT RECOGNITION AWARDS



Project Title: **ShowMe Your ID! – Missouri IAM**

State: Missouri

Agency/Division: Office of Administration, Information Technology Services Division

Award Category: Cybersecurity

Project Dates:
November 2022 – May 2023

Contact:
Paula Peters, Deputy CIO
State of Missouri
paula.peters@oa.mo.gov

Executive Summary

Early in Governor Mike Parson's administration as the 57th Governor for the State of Missouri, an emphasis was put on "Missouri Better Government". The Governor challenged State employes to "meet Missouri citizen's expectations so that we are good as any organization." There was an expectation that that Missouri state government become more transparent, more citizen friendly, more efficient, more focused, and more accountable. In response to this directive, the Information Technology Services Division (ITSD) at the State of Missouri began its journey to transform how Missouri state government serves its citizens using technology.

"Excellent citizens serving their fellow citizens."

-Governor Mike Parson

Missouri provides support to thousands of applications that impact the lives of millions of people. Many of these applications house highly sensitive data that require strict authentication and authorization protocols in place to access them. Given the sensitivity of the data stored inside these systems, they have become highly targeted by malicious actors. Phishing attacks against both citizen's and workforce to steal login credentials are a constant threat. Malicious actors target sensitive data to impersonate our citizens and make fraudulent claims or sell stolen information for personal gain. Unauthorized access by malicious actors allows them to disrupt Missouri business by destroying compromised systems or holding them for ransom. Any breach in security would tarnish Missouri's reputation and would certainly not be "better government". Authentication methods that only utilized a username and a password were no longer good enough to keep our citizen's data secure.

IDEA

With more sophisticated phishing attacks on the rise, Missouri identified a need to improve both authentication methods and user experience for both citizens and workforce. There was a need to act fast to protect applications and the data they hosted. It was decided that we would deploy an enterprise identity and access management system to address these security concerns with the implementation of multi-factor authentication and improve user experience through single sign-on. The scope of the project would include securing accounts for over 45,000 employees and 6 million residents across 1,300 applications by the summer of 2023. This solution would also help mature our security posture while enhancing our digital modernization efforts. Implementing an enterprise identity and access management solution also aligned with item number five of the NASCIO state CIO top ten policy and technology priorities for 2023. A very aggressive timeline was created to get this solution implemented across the state in a 6-month timeframe while limiting impact to citizen services and workforce access.

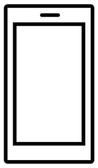
Multi-Factor Authentication (MFA)

Missouri recognized that old methods of authentication such as a simple username and password were not enough to protect this sensitive information and we needed to do better. We needed to incorporate an Identity Access Management (IAM) system into our framework. With IAM, we knew that we needed to deploy multi-factor authentication across our enterprise to protect our citizen's highly sensitive data. Research showed that over 95% of all authentication breaches are not using multi-factor authentication. This was a critical piece to securing our highly sensitive application data. When deployed, multi-factor authentication requires at least two forms of authentication to access a system. By enabling MFA, a malicious actor could no longer access sensitive data by compromising a username and password alone.   This greatly enhanced the security around the applications that house sensitive data.

Multi-factor authentication forms of authentication include the following:

Something you know: This includes items like a username, password, or personal identification number (PIN).

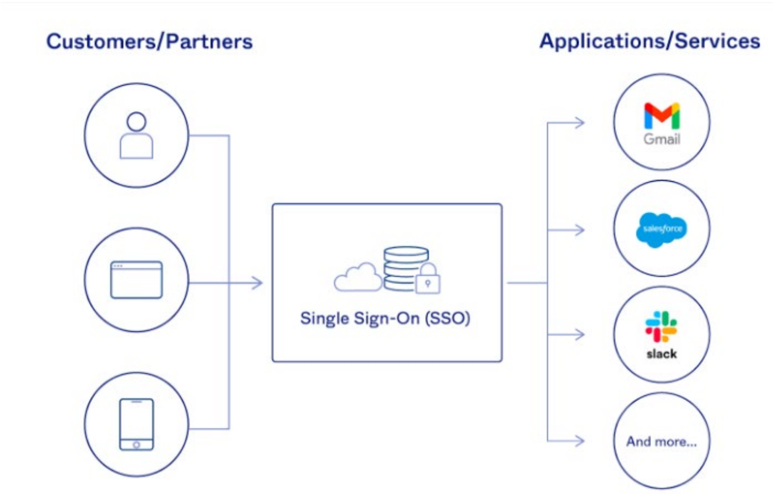
Something you have: These include a physical item like a cell phone with an application that can generate random tokens, or a physical token that does the same.



Something you are: This includes biometrics like facial recognition, voice recognition, thumb prints, handprint, palm scans, or retinal scans.

Single Sign-On (SSO)

Missouri also recognized the need to simplify user experience while improving the security around authentication. Our citizens and employees have access to multiple systems and each application required separate authentication. This made accessing multiple systems by the same user cumbersome and required them to remember how they authenticate into each system and must connect using that method each time they switched to a different application. By implementing single sign-on, a user would only need to sign in one time to access many applications that they had authorization to. This simplified the user experience. It also enhanced security because we could then enforce better password policies on the single authentication and enforce multi-factor authentication. Users no longer had to remember multiple usernames and passwords to log into each system. Password management was centralized which simplified the management of application passwords. It also simplified the on-boarding and off-boarding process for users' accessing these systems and allowed for centralized audit logging.



IMPLEMENTATION

Roadmap

Missouri adopted the NIST 800-53 cyber security framework. Implementation of an enterprise IAM solution aligned with the Identify and Protect pillars of this framework and was identified as a risk that needed to be addressed by our CISO in 2022. It was a part of our Digital Government Transformation efforts and was made an Office of Administration, Information Technology Services Division initiative item and received Governor Parson's support. Funding was approved and planning design started in November of 2022. Implementation started in December of 2022 and full enterprise roll-out was completed by May 2023. Successful completion of the project included full implementation of MFA and SSO capabilities across the entire 45,000 members of the State workforce and the ability for citizens to register their own accounts into our enterprise IAM solution. Missouri became a model state for our peers due to an aggressive and nearly flawless roll-out of our enterprise IAM solution.

Design

Our journey started with a design session that kicked off in November of 2022. The team researched many vendors to determine which would be our best fit to move forward with. The team attended conferences and spoke to other groups who had gone through the same journey. After a lot of research, the team decided to move forward with Okta as our IAM solution.

> To succeed at solving complex security problems, including those that emerge in digital government transformation, you need to practice security architecture.
>
> *-Gartner*

Leadership Buy-In

Missouri’s leadership from the top down, including Governor Parson, fully backed the rollout of an enterprise identity and access management system. Governor Parson, legislators, our commissioner, Deputy CIO and other c-level leadership helped us procure a budget for the implementation. They also helped coordination of efforts by making this project a priority for all involved. Without top level leadership support this project would not have been possible.

Creation of IAM Team and Collaboration Efforts

Resources were pulled together to form a new identity and access management team to help build out the enterprise IAM solution. Missouri’s Office of Administration/Office of Cybersecurity dedicated three team members to support this project. This team collaborated with all areas of the Office of Administration and worked closely with our active directory team, application development teams, and helpdesk to ensure that the roll-out stayed on track and users received assistance when needed. This team coordinated with all of our consolidated and non-consolidated agencies.

Communication

One of the biggest hurdles identified was coordinating the implementation process with consolidated and non-consolidated agencies, with many of them having their own authentication methods in place. Communicating what was coming along with having top-level leadership support were key to the success of this project and allowed us to get full buy in from agency stakeholders. The IAM team along with leadership, hosted multiple informational meetings to educate agency shareholders on identity access management, multi-factor authentication and single sign-on. These meetings pointed out the benefits of added security and ease of use that their users would receive through implementations. Follow up meetings provided a tentative rollout plan so that efforts could be coordinated.

Workforce Education

The IAM team also pulled in additional resources from the Office of Cybersecurity to host dozens of training sessions with agency workforce to educate them how to setup multi-factor authentication and provided dates on when enterprise remote access services would require MFA. The workforce was also provided detailed instructions along with contact information if they ran into any issues.

Rollout

By May of 2023, Missouri had fully implemented an enterprise identity and access management system with MFA across the enterprise workforce of 45,000 employees to access our most critical applications. With support from our highest leadership, we were able to coordinate these efforts and fully implement the solution in under six months! When speaking with other organizations our size and complexity, it had taken many of them several years to accomplish this!

IMPACT

Prevention of Phishing Attacks and Credential Stealing

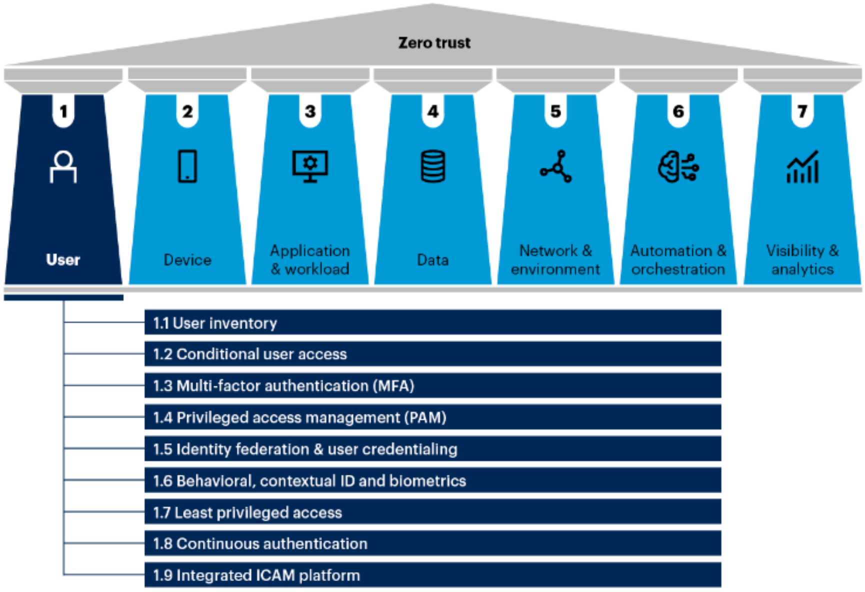
Malicious actors are constantly trying to find ways to steal sensitive information for personal gain. Phishing attacks are still one of the top attacks being seen in the wild today. A phishing attack involves a user being sent a malicious link to a fake website asking for credentials. It can then capture these credentials for the malicious actor to use on the real website.

Metrics on Missouri's e-mail security tools show that credential stealing phishing attacks against Missouri's workforce occur between 15,000-20,000 per month. Keep in mind that Missouri's workforce numbers are around 45,000 people and we are not able to see metrics for the personal email of our 6 million Missouri Citizens accessing State managed applications. Research performed by a security awareness training vendor showed that approximately 25% of people clicked on phishing attack links in 2022. If even 1% of those individuals entered their credentials, that has potential to impact 15,000 citizens. We implemented an enterprise IAM solution with MFA enabled on applications through credential theft; this greatly improved the security posture of the state of Missouri and helped us mature the identify and protect pillars of the NIST 800-53 cyber security framework that Missouri have adopted. This also aligns with Missouri's zero trust journey.

Reduced Data Breach Chances and Associated Costs

According to IBM's Cost of a Data Breach Report in 2023, the average cost of a data breach in 2023 was $4.5 million. This was a 2.3% increase over the 2022 cost of $4.35 million. According to Microsoft statistics, more than 99.9% of compromised account don't have MFA enabled. Applying IAM with MFA on Missouri's workforce side greatly reduces the chance of a data breach by preventing malicious access into systems that house sensitive data. Requiring MFA for system administrators with elevated access protects the data and systems that they are authorized to access. These are also required for the User Pillar of Zero Trust capabilities as defined by Gartner. (See figure to the right)

Zero Trust Capabilities Within the User Pillar


Zero trust
1
User
2
Device
3
Application & workload
4
Data
5
Network & environment
6
Automation & orchestration
7
Visibility & analytics
1.1 User inventory
1.2 Conditional user access
1.3 Multi-factor authentication (MFA)
1.4 Privileged access management (PAM)
1.5 Identity federation & user credentialing
1.6 Behavioral, contextual ID and biometrics
1.7 Least privileged access
1.8 Continuous authentication
1.9 Integrated ICAM platform

Source: Gartner, after U.S. DoD
804954_C

Reduced Attack Surface and Improved User Experience with Single Sign-On

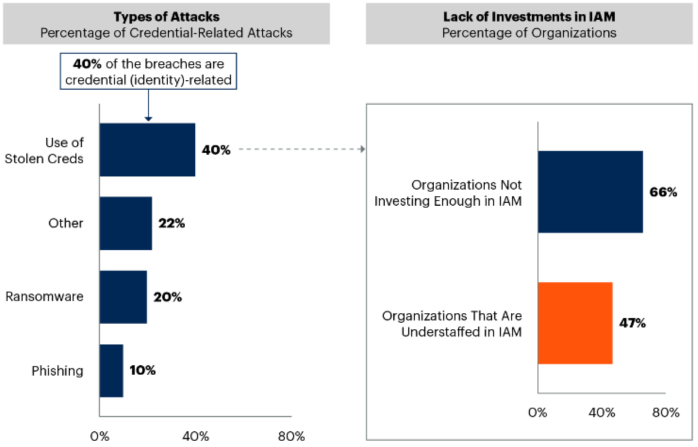
By implementing single sign-on (SSO) for Missouri applications we have reduced the attack surface to a single set of credentials. Combined with MFA, single sign-on makes it very difficult for a malicious actor to steal credentials. Prior to SSO, each application had its own authentication process. If a user jumped from one application to another, they had to login to each application individually. User experience was greatly enhanced because now a user of Missouri applications only needs to log in once to access multiple applications. Account management is now limited to a single set of accounts per user. This simplifies user on-boarding and off-boarding. Users can safely connect to their virtual desktops or to the state network using a virtual private network and efficiently access additional applications through SSO once the initial login and connection is established. The impact covers all 45,000 members of our state workforce and the 6 million citizens utilizing Missouri applications.

Workforce Testimony

Roll out of IAM with MFA and SSO has been well received by the State of Missouri workforce. System administrators no longer need to log into multiple systems throughout the day while authenticated to the State network from a State managed endpoint. They understand the importance of MFA and the security that it provides.

What Now?
Missouri is continuing to update its applications through digital government modernization efforts. The IAM team is continuing to assist with integrations into the enterprise IAM solution. Any new applications moving forward will be able to easily integrate and include MFA and SSO. Missouri is also rolling out it's citizen portal project where citizens can connect to a single website and access multiple State provided resources. IAM plays a major role in securing this portal and ensures that the citizen authentication experience is as seamless and secure as possible. We are currently working on identity proofing as an added layer of security to continue maturing the state's security posture. Missouri is also working on automating its user on-boarding and off-boarding process.

Return on investment of IAM, MFA and SSO
With increases in sophisticated attacks on the rise, security in layers is more important than ever. The value in rolling out an enterprise IAM solution can be seen by the lack of compromised accounts and stolen data. A single incident could cost the State millions in taxpayer money. To date we have not had a single incident of account compromise for an IAM managed account. (See figure to the right that shows the value of investments in IAM solutions)



Source: 2023 Verizon Data Breach Investigations Report; 2023 Gartner IAM Modernization Preventing Identity First Security Survey
Note: Percentages for credential-related attacks are shown as approximate values
IAM = identity and access management

Users no longer need to manage multiple user IDs and passwords. Having a single set of credentials to maintain with SSO implemented reduces calls to helpdesk staff for password resets. Having a single set of credentials to maintain streamlines user on-boarding and off-boarding process.

Missouri is also working on automating its user on-boarding and off-boarding process. According to Gartner, a company with 10,000 employees can realize a ROI of approximately 300% and save approximately $3.5 million over three years by switching to automated providing while utilizing an IAM solution. Using this as an estimate, Missouri can expect savings of approximately $15.75 million over three years once they complete the user on-boarding/off-boarding automation.