How State and Local Governments and Higher Education Can Achieve 100% Multifactor Authentication

Current and Former State Officials Share Their Experiences and the Best Path Forward for Planning, Communicating, and Funding

Jeremy A. Grant
Managing Director of Technology Business Strategy

Zachary P. Martin
Senior Policy Advisor

May 2022

VENABLE LLP

Introduction

Georgia Governor Brian Kemp knew that cybersecurity for the state was a priority. After a series of ransomware attacks the governor ordered semiannual cybersecurity training and then instructed the Georgia Technology Authority (GTA) to roll out multifactor authentication (MFA) for employee access to state networks.

As states face increasing threats and attacks, compromised usernames and passwords are still the primary attack vector.[1] Implementing MFA can go a long way toward securing state networks and applications, but it's not always easy. MFA is one piece of a larger identity and access management (IAM) platform that can be challenging to standup or upgrade. Figuring out which technology to deploy, which standards to follow, how to fund the projects, MFA requirements, and education of agencies and users are all challenges that state and local governments and higher education institutions face.

In Georgia, the direct intervention from the governor's office to use MFA for access to state networks and application meant that some of these typical challenges were overcome. When the governor asked GTA to improve authentication and add MFA, there wasn't the typical fight for funding that can happen in some states. With centralized IT operations in place with the GTA, it came down to choosing products that fit their needs and educating agencies and employees.

The GTA chose the YubiKey from Yubico, for phishing-resistant MFA, for those employees who didn't have state-issued mobile devices. The decision was based on positive consumer reviews and feedback from other organizations, such as the Gartner Group. Since November of 2020 the state has issued 30,000 YubiKeys to secure access to state networks and applications, according to Tanvir Doja, director of Infrastructure Services at the GTA. Okta is the IAM in place, and employees with state-issued mobile devices use the phone-based Okta Verify application, but more than half of state employees have a YubiKey for access, Doja adds.

At GTA, after YubiKeys were selected to complete MFA, it was a matter of educating agency officials. GTA and Yubico held education sessions with the state agencies, teaching them about the different YubiKey form factors, which form factor employees should choose, and how the keys work, Doja said.

A key to the successful rollout was getting buy-in from the different state agencies. Instead of presenting MFA as something that was being forced, GTA approached the agencies with educational materials and empowered them to make choices. "This was not presented as a mandate," Doja said. "We approached everything with the respect that agencies are still independent, and we wanted to get their buy-in."

Employees could choose from five of the most popular YubiKeys available, depending on which one best fit the way they worked. These ranged from YubiKeys that are plugged into a USB port for authentication – and support near field communication (NFC) for use with mobile devices – to smaller USB Nano series keys that remain in the laptop.

Since the program went live in November 2020, there have been minimal reported problems – one or two support tickets sent to Yubico. One of the few lessons learned was the need to revise the descriptions of the different keys so that employees have a better understanding of which one to order.

1 https://notified.idtheftcenter.org/s/2021-data-breach-report

Challenges for State and Local Jurisdictions

Support from government leadership – as shown in Georgia, with the governor leading the way – can enable identity projects to run much more smoothly. Senior officials can help prioritize funding and ensure buy-in from all necessary stakeholders. But not all states and local jurisdictions are as lucky as Georgia.

The lack of a statewide centralized infrastructure for managing digital identity can be problematic, particularly post-pandemic, as more workers need remote access to high-security systems to accommodate new working conditions. During the pandemic's peak in May 2020, 57% of the government workforce was teleworking.[2] As we begin to emerge from COVID-19, many are returning to the office, but telework is expected to remain an option for many in the public sector workforce. As of January 2022, 67% of agencies reported that up to 25% of their staff was still working remotely one to three days a week, with 43% stating that their office remote work policies have changed.[3]

Sixty-one percent of the security and IT leader respondents are concerned about an increase in cyberattacks targeting their employees who are working from home.[4] Securing this workforce is critical, and the first step is to add MFA, to make sure abuse doesn't come through the front door.

Last, as ransomware incidents explode, insurers are asking more questions before underwriting policies.[5] MFA implementation is near the top of that checklist, and without it some organizations can see their premiums as much as double.[6] Phishing-resistant MFA needs to be at the top of CISOs' checklists when it comes to security improvements.

Georgia officials knew steps needed to be taken to secure their infrastructure with MFA. But not all MFA is created equal, and state and local jurisdictions have other challenges to overcome before the security technology can be implemented, including:

- Obtaining funding
- Choosing products that adhere to government policies, standards, and best practices
- Gaining stakeholder buy-in

Funding

State IT budgets can be tight, and MFA is not always baked into the per-user cost that state agencies pay to the central IT services organization. States may offer a centralized enterprise identity and access management and directory services, but not necessarily MFA. This leaves each agency to make that decision and come up with the additional funding.

When New York State switched to centralized IT services, access management posed an interesting challenge for the new agency, said Deb Snyder, former New York State chief information security officer. "The challenge was that identity management, or access management specifically, was embedded in apps; with multiple directories per agency and was very fractured," she explained. "Fortunately, in New York State, we gained budget funding to support centralizing identity and access management. So, we built out the platform and components, to support the identity management lifecycle - identity store, directory consolidation, process flows for provisioning/deprovisioning - creating identity management as a service."

2 https://www.govtech.com/biz/data/survey-shows-many-government-employees-still-teleworking
3 https://www.prnewswire.com/news-releases/springbrook-research-institute-survey-finds-local-government-agencies-faced-multiple-technology-challenges-during-pandemic-301503451.html
4 https://www.cisecurity.org/insights/white-papers/resource-guide-for-cybersecurity-during-the-covid-19-pandemic
5 https://www.governing.com/security/can-government-still-afford-cybersecurity-insurance
6 https://www.crcgroup.com/Tools-Intel/post/multi-factor-authentication-a-must-have-for-cyber-coverage

When it came to MFA, finding the funding was hit or miss. "The focus was on agencies that had the money to cover licensing and deployment of MFA," Snyder said. "If agencies had funding for a critical initiative, you likely had money to deal with identity access management. If you didn't, then it was anybody's guess whether the project budget provided for it, which resulted in a fractured dialogue."

To apply for funding, states will need to make a business case. This typically is a two-step process; one business case is needed for state leadership on why the technology is necessary, and the other is needed to obtain grant funding from federal agencies. Still, with limited resources, elected officials will ask many questions. "Why is it so important to the portfolio as a whole?" asks Phil Bertolini, former CIO and deputy county executive for Oakland County, Michigan. "What are the security components that this solves? What are the other issues that this takes care of for all of our operational systems? Are they able to access the technologies they need from a remote location to be able to do the work they need to do for the people? All of those issues are a huge struggle for local government."

Justifying the cost is critical, Bertolini adds. "I need to do an enterprise-level IAM to make sure we're keeping all of our systems safe, and the elected officials say, 'Wait a minute, we just argued over paying $1000 for an electric bill. Now you want to spend $50,000 on an IAM? What's that going to do for us?'"

A three-year strategic plan is a good baseline for officials and supports grant applications, Snyder said. "You need a strategic plan with targeted, prioritized initiatives that move you from where you are right now - based on an assessment of current state - to where you want to be - your target state. And then, where feasible, tie prioritized initiatives back to federal funding opportunities. Clear use cases and cost benefit analysis are essential to success in getting grant funding."

Here's the Great News:

There is now significant federal grant money available to support state MFA implementation, thanks to the American Rescue Plan (ARP) and the Bipartisan Infrastructure Law. Almost $2 billion was allotted for cybersecurity, with a large allotment for the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) to distribute $1 billion over four years to state and local governments.[7] Additionally, the ARP provides $350 billion in funding that may be used for cybersecurity, including modernization of hardware and software.

The first of these grants are expected to be issued in the summer of 2022, with $200 million to be granted before the end of the government's fiscal year on September 30. With the federal focus on zero trust and phishing-resistant MFA, citing adherence to these technologies may give jurisdictions an advantage when it comes to grant funding. States and local jurisdictions should work with vendors and systems integrators to find out how the products and systems align with federal policies and standards and cite that in their grant applications.

It depends on the grant vehicle, but they are typically awarded to specific state agencies, said Snyder. Where state IT services are delivered through a shared service model, agencies may be charged a flat or per-employee rate for email, office applications, and other services. Something like basic identity management services may be baked into the overall user support cost, but adding MFA may be an additional cost. "The exception might be where the IT organization works with the Department of Homeland Security to obtain grant funding specifically tagged for infrastructure improvement modernization, IT modernization, and cybersecurity," Snyder explained. "But for the most part, many states are still hitching their wagon to agencies that have funding for system and program enhancements."

Local governments can find obtaining funding for some of these projects difficult too. There may be some instances of states offering shared services to county and local governments for a fee; however, these have been

7 https://statescoop.com/state-local-cyber-grant-program-summer-cisa/

limited but have expanded in the last few years, Snyder says. "We saw this in 2016, with the focus on election security," she explained. "There were initiatives like monitoring services and risk assessments, where a contracted entity helped local districts assess whether appropriate controls were in place for elections systems, and continuous monitoring and alerting services were made available."

To help reduce costs, smaller organizations can use contracts and procurement vehicles that a state has in place to purchase services and MFA, Snyder says.

Choosing the Right Authentication Solution

The strategic plan used to obtain grant funding will identify the systems that need to be updated but not necessarily identify specific products. Before choosing products, state officials should make sure that they align with federal standards and policy.

Adding MFA may seem somewhat simple, but not all modalities are created equal. As adoption of MFA has increased, so have the attacks against the security technology. One of the biggest vulnerabilities with legacy mobile-based MFA – SMS, one-time passcodes, and mobile app-based systems – is that they are increasingly easy for attackers to phish. This has left both the Cybersecurity Infrastructure Agency (CISA) and the White House Office of Management and Budget (OMB) to mandate that federal agencies deploy phishing-resistant MFA to combat these more sophisticated attacks, and CISA states that PIV Smart Cards and the Fast Identity Online (FIDO) specification – which Yubico helped create – are the only phishing-resistant authentication standards. Furthermore, they state that FIDO2 is the "gold standard" for MFA.[8]

Phishing attacks are where legacy MFA falls short and increasingly puts state agencies at risk. For example, with legacy MFA like one-time passcodes or push-based systems, a state worker might get an email with a link to a document on a file-sharing site from a "coworker." The worker clicks on the link and is prompted by the attacker for their username and password to their state network. After entering that information, they are prompted by the attacker for the one-time passcode from their mobile device, which they enter. Or if an app-based tool is used, the worker might get a prompt from a push notification on their mobile device. In either case, the worker has been tricked into bypassing MFA. The login page then shows an error, but it's too late as the email was part of a phishing campaign, and now the attacker has access to the state network.

Phishing-resistant MFA, based on public/private key cryptography, reduces the attacker's ability to intercept and replay access codes, as there are no shared codes. Additionally, the authentication action can occur only between the user's device and the site they are visiting. The phishing-resistant technologies specifically mentioned in the OMB's Zero Trust Strategy are PIV Smart Cards and the FIDO2 WebAuthn standard.

The OMB Zero Trust documentation is one that states should align with, but there are other guidelines too, including those from the National Institute of Standards and Technology that can be used to guide states in their implementations.

8 https://www.cisa.gov/mfa#:~:text=FIDO%20Key%3A%20FIDO%20stands%20for,all%20major%20browsers%20and%20phones.

Table 1: Federal Policies and Guidelines		
	Document	Description
1	**Digital Identity Guidelines, NIST Special Publication 800-63-3**	The four-volume guidelines detail requirements for identity proofing and enrollment, authentication and lifecycle management, and federation and assertions. A draft of 800-63-4 is expected at some point in 2022.
2	**Executive Order on Improving the Nation's Cybersecurity**	A broad set of new cybersecurity policies, including zero trust, system monitoring, and information sharing, among others.
3	**Zero Trust Strategy, M-22-09**	More detailed guidance that was first mentioned in the cybersecurity EO. Specifically cites that federal agencies must use phishing-resistant MFA.
4	**Criminal Justice Information Services (CJIS)**	The FBI requires that anyone accessing CJIS uses MFA.

State adherence to federal policies and standards can be hit or miss. Some states will see what's coming and plan, while others will wait until there's a regulatory requirement that compels adherence via an audit. "Anything that is downstream from a federal oversight, federal funding, federal programmatic perspective, and there's touch points with federal data, they're going to expect you to comply with their regulations," Snyder says.

As for the Zero Trust Strategy, Snyder said that state and local governments will find the recently released federal guidance useful in their efforts to secure and modernize their systems. "This is an aggressive and robust set of directions on how to implement," Snyder added.

Educating Stakeholders

After funding and choosing products that fit the needs of your agencies and meet policies and standards, then it's a matter of educating stakeholders. "As new services came online and were available, the communications and customer relations staff got together, wrote the communiqué that went out to all of our agencies and partners talking about it, and then we did a little bit of a tour," Snyder explained. "We went agency to agency, talked about it at various meetings, to make sure stakeholders understood how it functioned and the business value it provided."

While in most cases, actions taken to make your systems more secure would be well received, the work or impact the system owners need to invest to achieve that level of security may not be, said Brian Cohen, former vice chancellor and chief information officer for the City University of New York (CUNY). The University rolled out an enterprise IAM and MFA policy during Cohen's tenure, and the response from stakeholders was mixed.

System owners were asked to assess their systems and determine the level of risk associated with the data stored within, Cohen said. "We inquired about the type of data in the system and how sensitive the data was – PII vs. confidential, vs. high risk. We wanted them to have a better understanding of the impact if there was breach. Afterall, no system's owner wants their systems on the front page of the local newspaper," he added.

While the approach might seem a bit harsh, the goal was to elevate the importance of securing data to system owners and the implications of not taking the necessary steps. "Not everything needs MFA, but it is important to engage business owners in the process and decisions required; they needed to be part of the University's analysis and decision making," Cohen says.

The next challenge at CUNY was to engage the users - faculty, students, and staff. "Most people were not provided CUNY-issued cell phones and had to use their personal devices to authenticate when logging in. Our user base is also so diverse in their own technology, that many still had flip phones, do not have or use text messaging, and were also not able to access or want to download an authenticator app," Cohen says.

To fill this gap, CUNY deployed an MFA approach that used multiple modalities, including one that enabled a voice call to relay an OTP, Cohen explained. "We knew this approach would allay many fears since it used a similar approach that many of our users were already used to from an everyday perspective," he said. "Our approach was no different than how they may log into their bank accounts – a text, an email, or a phone call. In the end, we wanted them to know that we are taking the same steps to protect their data in our system."

Conclusion

Implementing MFA for a state or local government or higher education organizations is a multistep process that involves the following:

- Creating a strategic plan and business justification for the cost is a critical first step
- Identifying federal grants that can help fund the MFA
    - Ensuring grant applications is making sure they align with federal policies and standards – phishing-resistant MFA and zero trust
- Picking products that align with those policies, leveraging infrastructure in place today, and solving the agency risk tolerances:
    - Unify the identity infrastructure to shrink the attack surface
    - Provide authenticator options dependent on risk tolerances, as not all MFA is created equal:
        - Legacy mobile-based MFA like OTP and push are frequently getting phished
        - MFA utilizing FIDO security keys such as YubiKeys stops phishing attacks
- Communicating with stakeholders and rolling the new system out in a way that makes them feel heard and clearly explains what's happening

VENABLE LLP