yubico

WHITE PAPER

Modernize authentication across state, local, tribal and territorial governments

Close authentication gaps and drive 100% MFA

Table of contents

Uptick in threats across state, local, tribal and territorial (SLTT) governments

State, local, tribal and territorial (SLTT) governments are increasingly the target for cyber attacks due to highly sensitive information they hold and critical services they provide or oversee such as utilities, emergency services including fire and police, education, the judiciary, healthcare services, and election systems. Further, the past three years have forced a radical transformation across the more than 90,000 government organizations[1] in the US in order to support new digital and mobile services and new levels of remote and hybrid work—transformations that have increased the risk of cyberattack.

The average cost of a data breach in the public sector is $2.07 million in 2022, with the cost of incident response and recovery often representing the bulk of that cost.[2] Notably, the city of Atlanta spent over $2.6 million to recover from its ransomware scare in 2018, of which only $52,000 was attributed to the ransom payout.[3] According to a 2020 study, ransomware attacks on US government organizations exceeded $18.9 billion across the sector.[4]

The consequences of a cyberattack can be catastrophic when they involve disruptions or shut-downs of critical services and infrastructure or threats to the election ecosystem. Modern cybercriminals target local governments with the aim to steal information and to impede their ability to function. In 2021, for example, an attack on a water treatment plant in Oldsmar, Florida was stopped in real-time as an intruder attempted to introduce dangerous levels of sodium hydroxide into the water supply.[5] In March 2022, the FBI warned of increased levels of ransomware attacks against SLTTs that have resulted in "disrupted operational services, risks to public safety, and financial losses."[6] According to a recent Deloitte-NASCIO Cybersecurity Study, "local governments present a threat vector" to all levels of the government due to the many interactions that take place between state and local agencies.[7]

The critical need to restore services quickly along with a lack of cybersecurity funding and staff contribute to local governments being seen as "low hanging fruit" for attacks. According to a nationwide cybersecurity survey of local governments, 28% report being attacked at least hourly—yet only 48% had adopted cybersecurity policies and standards countywide.[8] Further, there has been a steady rise in phishing aimed at government agencies, with 50% of phishing attacks designed to steal credentials.[9]

With the rising rates of cyberattacks, both regulations and cyber insurance requirements are pushing SLTT government organizations to adopt phishing-resistant multi-factor authentication (MFA) as a baseline cybersecurity precaution. But historically there have been barriers to adoption from a lack of IT staff to budget pressures. Thankfully, the Department of Homeland Security (DHS) recently announced a new cybersecurity grant program specifically for SLTT governments. The State and Local Cybersecurity Grant Program makes $1 billion available to help state and local governments become more resilient to attack.[10] According to a recent survey, 35% of states will require local governments to implement multi-factor authentication to receive funds under this grant.[11]

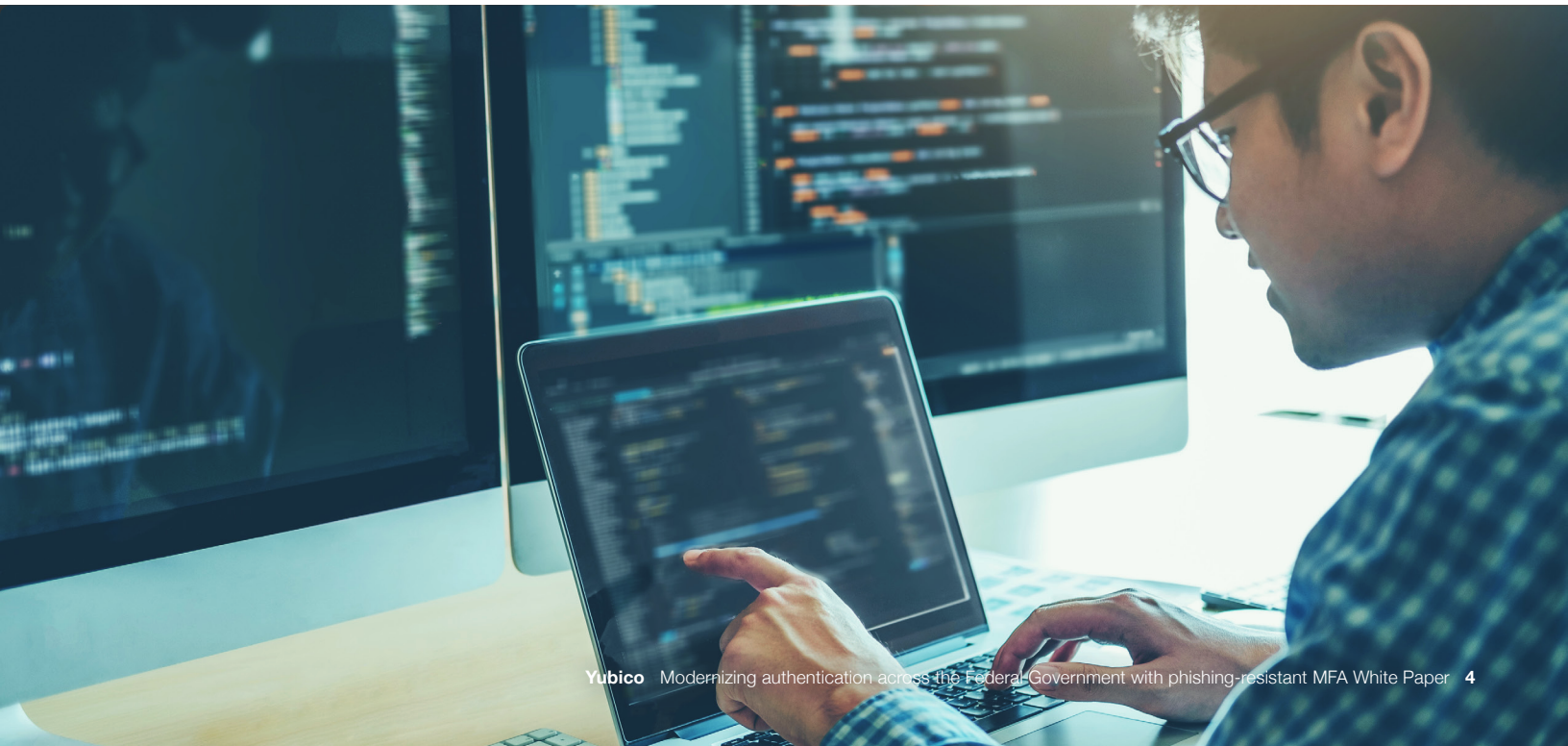
> Having strong authentication is a foundational security component of a Zero Trust architecture. Yubico and YubiKeys help fill the gap, for example, where weak passwords have been used, by providing validated, phishing-resistant security keys."
>
> —John Kindervag
> Creator of Zero Trust

Increasing regulatory compliance burden

In an effort to better protect citizen data and critical services, an increasing number of data privacy and data security standards and regulations have emerged. At the state level, this includes new stringent requirements such as the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (VCDPA) and varied compliance obligations including the Health Insurance Portability and Accountability Act (HIPAA), the FBI's Criminal Justice Information Services (CJIS) Security Policy, the PCI Data Security Standard (DSS), and IRS Publication 1075 Tax Information Security Guidelines for Federal, State and Local Agencies. Common across all these regulations is the requirement to ensure the privacy and security of protected information, many of which are based on the NIST Cybersecurity Framework.

In 2021, President Biden issued an executive order (EO) on improving the nation's cybersecurity (EO 14028) for federal agencies, outlining key areas that need to be addressed to protect critical digital infrastructure.[12] The order and subsequent OMB Memo M-22-09 mandate the requirement to adopt phishing-resistant MFA as part of deploying a Zero Trust Architecture.[13] While the mandate impacts federal agencies, it is prudent to expect that it will have a trickle down effect on SLTT governments. In fact, the State and Local Government Cybersecurity Act of 2021 codifies the relationship between federal and SLTT governments in helping address cyber incidents.[14]

Zero Trust urges organizations to trust no one or no thing unless properly verified before being given access to sensitive resources. Phishing-resistant MFA refers to an authentication process that is virtually immune to sophisticated attacks that could intercept or trick users into revealing login credentials. As defined by the Federal Information Processing Standards (FIPS) 140-2 and NIST SP 800-63B, only two authentication technologies currently meet this requirement: the federal government's Personal Identity Verification (PIV) standard/SmartCard and the modern FIDO2/WebAuthn standard.

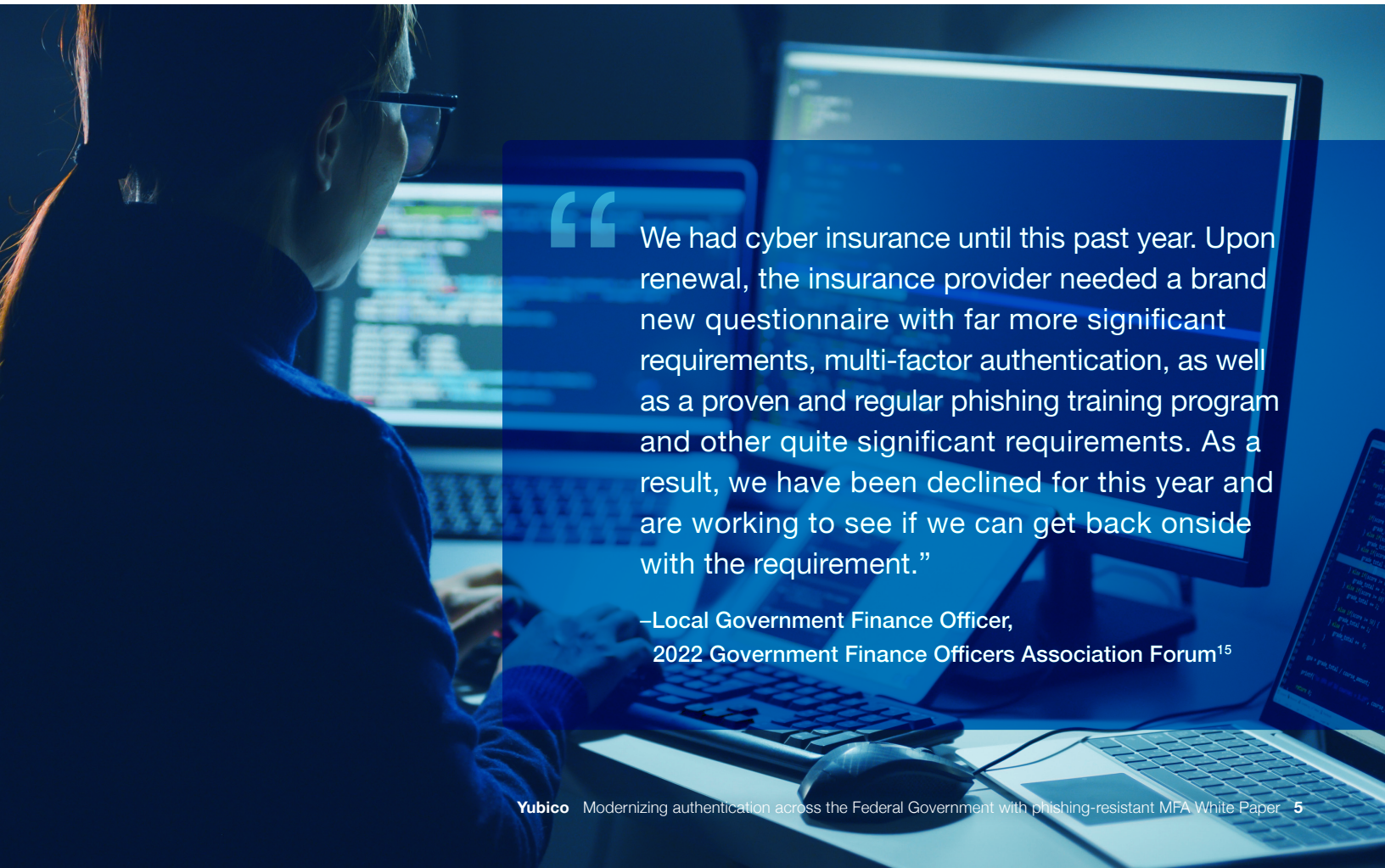


Increasing threats impact cyber insurance

In response to the uptick in the number and sophistication of cyberattacks, cyber insurance risk models have had to adapt—it has simply become too easy for an attacker to steal user credentials and work from the inside to steal information or impact operations. The heightened risk profile of recent attacks has resulted in higher premiums, some in the range of 150-300% higher, or added restrictions including reduced sublimits, higher deductibles and narrower coverage terms.

The cyber insurance industry is still developing in response to new threats and new demand for coverage, but the basic tenet of insurance still holds: those organizations at the highest risk will pay the highest premiums—or might not qualify at all. Most cyber insurance coverage will come with a cyber risk vulnerability report that mirrors the latest federal standards set out in Biden's Executive Order. The requirement for phishing-resistant MFA will become the de facto standard for government agencies—both to comply with the EO and to qualify for cyber insurance.

States, cities, and counties can face a shortage of cybersecurity insurance capacity and increased cost for coverage if MFA isn't satisfactorily deployed across the entire ecosystem. Cyber policy non-renewals may also be a potential outcome, which can expose an organization to significant risk if targeted by hackers, phishing attacks or ransomware attacks.



> "We had cyber insurance until this past year. Upon renewal, the insurance provider needed a brand new questionnaire with far more significant requirements, multi-factor authentication, as well as a proven and regular phishing training program and other quite significant requirements. As a result, we have been declined for this year and are working to see if we can get back onside with the requirement."
>
> –Local Government Finance Officer,
> 2022 Government Finance Officers Association Forum[15]

Risk of account takeover rates

0%

FIDO security key (YubiKey)

10%

On-device prompt

21%

Secondary

24%

SMS Code

50%

Phone number

Account takeover prevention rates
Google: How effective is basic account hygiene at preventing hijacking

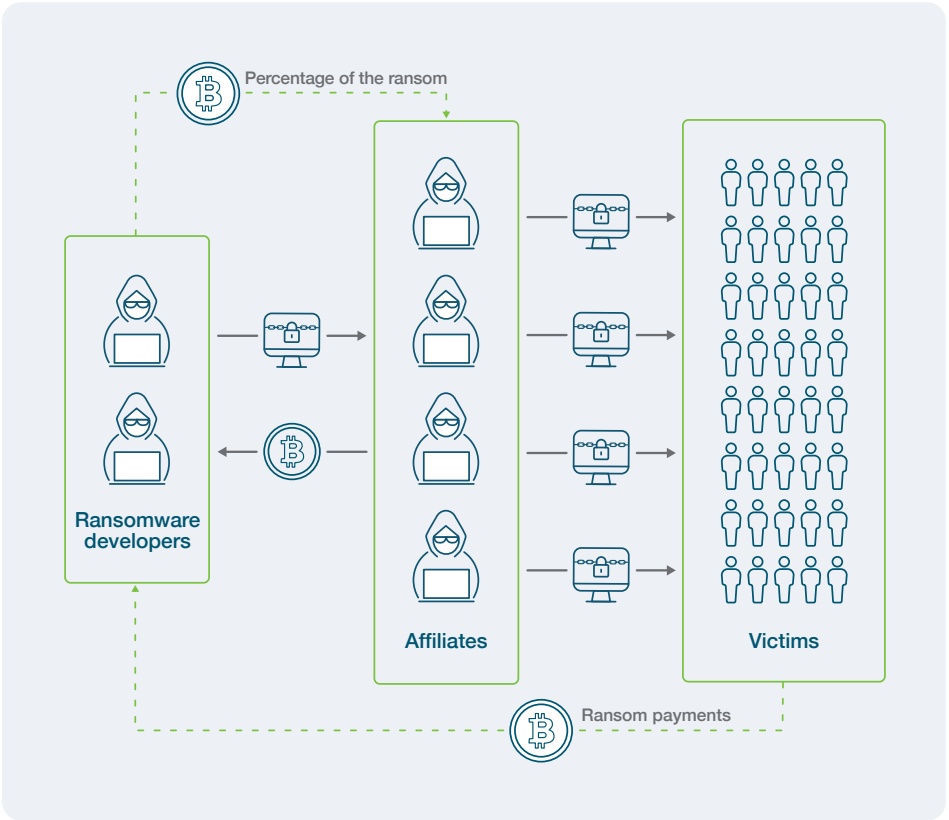
Drawbacks of legacy authentication

Prior to COVID-19, and even today, there are many state and local governments that are still relying on usernames and passwords for authentication. While SLTT may prioritize or even mandate stronger MFA protection with mobile-based MFA such as SMS one-time passcode (OTP) or push apps, there are almost always MFA gaps created when users can't, won't or don't use mobile-based MFA. These edge cases include restrictions imposed by unions on employees using personal mobile devices for work purposes, users that don't have smartphones, users who live in remote geographic areas that have low cell coverage or users that won't use their personal mobile devices, creating MFA gaps if the fall back authentication method is just username and password.

Security

When adopting cloud services, federal agencies pay careful attention to cybersecurity While any form of MFA offers more security than passwords alone, each still relies on passwords as the first factor. Further, mobile-based MFA ties the second factor to the mobile device, which offers no guarantee that the private key ends up on a secure element on the mobile device, the OTP code or private key could be intercepted in some way, and it is impossible to ensure proof of possession; or in National Institute of Standards and Technology (NIST) terms—impossible to prove it is phishing resistant.

Phishing-resistant authentication can put a halt to ransomware entry that relies on stolen or phished credentials. Here is how phishing-resistant MFA stops a ransomware attack:



A ransomware attack is the result of a chain of events, and not a singular event. That chain of events begins with infiltrating the SLTT government or one of its supply chain partners through stolen credentials, a phishing attack (often also targeting credentials), or a direct attack. In the case of stolen credentials, the attacker virtually walks in disguised as a legitimate user, making this type of attack difficult to detect.

Once inside, the attacker has a path to collect sensitive and confidential before "executing" the ransomware attack. Thus, the best way to combat the growing threat of ransomware is to improve patching and to implement phishing-resistant MFA so that attackers cannot steal credentials as easily as they do when passwords or legacy MFA such as SMS and mobile authentication apps are in use across the organization.

User Experience

Beyond security, legacy mobile authentication creates friction in the user experience if users are not able to seamlessly authenticate. Authentication is a mission-critical service, and if users can't log into the apps or devices they use, they can't do their job. For SLTTs that provide critical emergency services or who maintain critical infrastructure, including first responders, the need to authenticate quickly in the field cannot be tied to common points of failure related to connectivity, device battery, cell reception, hard token battery, or even a password. These users need secure and speedy access to machines, VPN and Criminal Justice Information Service (CJIS) systems to be able to operate quickly and effectively.

IT Burden

The lack of cybersecurity professionals and staff remains one of the top barriers to responding to rising threat levels, particularly in the face of much faster-paced hiring cycles in the private sector. Any form of legacy authentication such as usernames and passwords, and mobile authentication applied and enforced at scale, will require ongoing policy enforcement, user training and IT support. It's important to note that legacy mobile-based 2FA and MFA create a huge support burden if codes are delayed, users get locked out of their accounts and require help, or users need to register new devices.

Due to the high IT burden and poor security of legacy authentication, SLTT governments should consider moving toward passwordless authentication—authentication that does not require the user to provide a password at login.

FIPS

YubiKeys work with more than 1,000 applications and services out-of-the-box

DUO
PING
Microsoft
okta
Google

YubiKeys offers modern, phishing-resistant authentication for SLTT governments

The YubiKeys is a FIPS 140-2 validated hardware security key, manufactured by Yubico, that offers easy-to-use two-factor, multi-factor, and passwordless authentication at scale. The YubiKey is the only solution that is proven to stop 100% of account takeovers in independent research.[16]

The YubiKey uses modern protocols such as FIDO U2F and FIDO2 open authentication standards and additionally support protocols such as OPT, smart card and OpenPGP, with the hardware authenticator protecting the private secrets on a secure element, entirely eliminating phishing-driven credential-based attacks and supporting a user-friendly login flow. The YubiKey is user-friendly, cost-effective and can serve as a critical enabler of a zero trust security architecture.

More importantly, the YubiKey helps close any MFA gaps for any users that can't, don't or won't use mobile authentication due to union restrictions, personal preferences, cellular geographic inconsistencies, financial reasons or more. A single YubiKey works across multiple devices including desktops, laptops, mobile, tablets, notebooks, and shared workstations, enabling users to utilize the same key as they navigate between devices. SLTT governments can simplify hardware management because keys can easily be numbered, tracked and managed. YubiKeys are also easily re-programmed, making them suitable for temporary or contract staff.

- **4x faster logins**
- **Zero account takeovers**
- **92% support reduction**
- **Single key across legacy and modern infrastructures**
- **Meet cyber insurance mandates**

The YubiKey can be deployed in-person or shipped directly to remote and hybrid employees, with the option for admins to pre-enroll users or allow for self-enrollment via a web portal. YubiKeys integrate seamlessly with existing identity and access management (IAM) and identity provider (IDP) solutions such as Microsoft, Okta, DUO, Ping, and more than 1,000 applications and services out-of-the-box, including Google Suite, Microsoft Azure, Microsoft Office 365, Box, Jamf, and identity and credential management (ICAM) solutions, eliminating rip and replacement of existing solutions.

The future is passwordless

Ultimately the actions of the user are the biggest weakness in conventional authentication such as passwords, and multi-step authentication is a big contributor to user dissatisfaction, which is why the global best practice is moving toward passwordless authentication—authentication that does not require the user to provide a password at login.

While moving from legacy MFA to passwordless authentication may seem like a big jump, it's a jump that completely bypasses the unnecessary dissatisfaction found with more conventional MFA methods and offers a solution that can bridge both legacy and modern environments.

The FIDO modern authentication standard enables strong two-factor, multi-factor, and passwordless authentication. FIDO2/WebAuthn is the most recent iteration of the FIDO standard, and uses public key cryptography for high security, where the private keys never leave the authenticator, enabling modern two-factor, multi-factor and even passwordless authentication to help get SLTT governments to 100% MFA at any stage.

> I like the YubiKey as opposed to phone authentication. We have a lot of users within our system that don't have a state- or county- provided cell phone, and I certainly don't want them using their own personal devices for agency or office business. The YubiKey was really the easy-to-use multi-factor authentication of choice for us here in Washington state to achieve the additional security needs we had."
>
> **Lori Augino, Elections Director, Washington State**

Common authentication scenarios supported by the YubiKey

With the YubiKey, SLTT governments can deploy highest-assurance, phishing-resistant MFA to support a variety of authentication scenarios, including:

Email & cloud-based / productivity applications

Many SLTT government systems and applications contain sensitive information, including personal identifiable information about citizens and staff. With the shift to remote work and cloud-based productivity applications, governments need a way to secure remote access to corporate networks, protected resources or access from unsecured home or public networks and employee-owned devices.

The YubiKey secures remote access by enabling phishing-resistant 2FA or MFA for leading VPN applications, remote access applications, Identity and Access Management (IAM) and Identity Provider (IdP) platforms to enable employees to work without the hassle of multiple usernames and passwords.

The YubiKey is natively supported by leading IAM platforms (Microsoft, Google, Okta, Duo, Ping) to provide federated access to web applications and service-related apps and can be used for single sign on (SSO) to messaging and video conferencing apps such as Microsoft Teams, Google Hangouts and Zoom.

The YubiKey can authenticate to existing Microsoft users, either Azure, Azure Active Directory (Azure AD), or Microsoft 365, can take advantage of native support for the YubiKey for immediate compliance with the authentication requirements of OMB M-22-09 in a Zero Trust framework.

80%

Forrester estimates that 80% of data breaches have a connection to compromised privileged credentials.[17]

Privileged access / high-security applications

Privileged users have elevated access to systems, software, data or infrastructure. They include privileged IT users such as engineers, IT admins, security admins, network or database admins, privileged business users in HR, finance, or users in judicial systems or policing who have access to sensitive or confidential information.

New and varied threat vectors put privileged users at great risk. Forrester estimates that 80% of data breaches have a connection to compromised privileged credentials.[17] Compromised credentials provide ready access to sensitive information such as budgets, planning documents and PII/PHI, which can have a crippling impact on the government.

YubiKeys bridge legacy MFA to modern protocols such as FIDO2 and WebAuthn. The YubiKey's hardware design enables the authentication secret to be stored on a separate secure chip built into the YubiKey, so it cannot be copied or stolen. This offers the highest security for authenticating privileged users.

The YubiKey can be used as an additional form of validation for high-security applications, to quickly re-verify the user before access is granted or a required action is taken. Learn more about the critical strong authentication needs for privileged users.

Workstation login

Shared workstations are common for citizen-facing government services, including libraries and services such as licensing and records. Shared workstations amplify the insider threat, whether malicious or negligent, and present additional security risks when used in high-traffic areas.

Government workers that use shared devices/workstations can benefit from a portable root of trust. The YubiKey is an extremely robust and reliable solution, offering high security and exceptional user experience, replacing time-consuming and insecure mobile second factors with a consistent tap-and-go experience.

Public works

Local governments are responsible for public works, supporting a highly mobile workforce of public works professionals who build, operate and maintain critical infrastructure and services. Beyond protecting the integrity of these systems, public works professionals need access to data, services and systems to enter notes in the field, support communication and quickly respond to constituent needs. For example, many local governments rely on geographic information system (GIS) technology across a variety of services, including permitting, police and fire, water and waste management.

The YubiKey provides these employees with a way to securely access systems from mobile devices, both government and employee-owned, or to authenticate to systems in off-site or secure locations without reliance on a mobile device, which may be down or unavailable.

First responders / emergency services

State and local governments are responsible for a wide range of emergency services across city police departments and fire stations, county sheriff's offices and emergency medical providers. As noted above, paid and volunteer first responders need critical field access to GIS and first responder software to view up-to-date information about 911 calls, edit field data, and search records to support response efforts.

Policies set for by the CJIS security policy requires MFA when accessing criminal justice information and for all persons who administer or maintain systems or data. A YubiKey helps meet CJIS Advanced Authentication requirements (section 5.6.2.2), providing highly portable, secure access to critical data for emergency operations. Further, the YubiKey does not rely on mobile connectivity or battery life, making it a reliable point of connection in the event of a natural disaster or disruption to network connection. The YubiKey works with any major laptop, desktop or mobile device, including the Toughbooks in use across first responder vehicles.

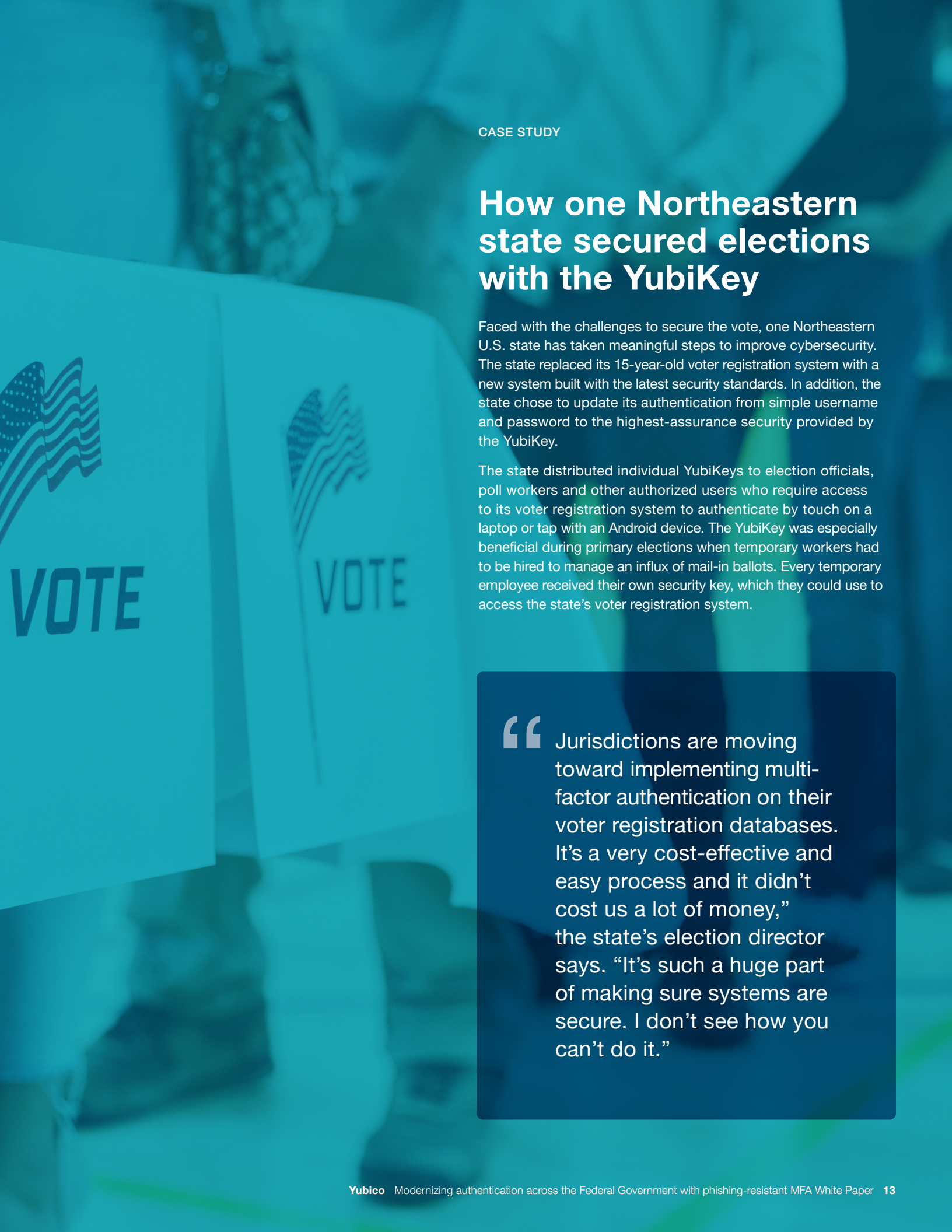
> "While the attackers might be the same—we will definitely see nation states and cyber criminals and hacktivists—their motivations to attack a specific campaign would be greater than, say, an attacker who is probing networks, looking for someone who didn't patch for the latest version of Windows."
>
> —Michael Kaiser
> President and CEO Defending Digital Campaigns Inc[18]

Elections infrastructure

Safe, fair and secure elections are the bedrock of America's political system, but states throughout the country face increasing challenges protecting their elections. The election ecosystem is a prime target for cyber threats, including voter registration databases, voting results databases and poll books. Further, elections heavily rely on temporary workers and portable devices such as iPads and tablets to support shift work. Combined with aging voting infrastructure, it's never been more crucial for states to strengthen their security posture and increase voter confidence that the voting process is secure.

YubiKeys can be distributed to election officials, poll workers and other authorized users who require access to voting systems, complying with the US Election Assistance Commission recommendation that only authorized personnel should have access to the voter registration database. Each user can be assigned a unique registered key that can be used as a second factor, inserted into a USB port and touched to log in. The user's touch serves as verification that a human—and not a remote hacker—is trying to access the system. Since the YubiKey is portable, it allows election officials, registrars and poll workers to use different devices and systems simply entering their credentials and using this one-touch solution.

Further, as past elections have seen hackers compromise social media accounts connected to campaigns and elections. YubiKeys can enable strong verification of election officials and nominees before providing access to their social media accounts—even if a user is tricked into giving up their username and password, the YubiKey isn't fooled.



CASE STUDY

How one Northeastern state secured elections with the YubiKey

Faced with the challenges to secure the vote, one Northeastern U.S. state has taken meaningful steps to improve cybersecurity. The state replaced its 15-year-old voter registration system with a new system built with the latest security standards. In addition, the state chose to update its authentication from simple username and password to the highest-assurance security provided by the YubiKey.

The state distributed individual YubiKeys to election officials, poll workers and other authorized users who require access to its voter registration system to authenticate by touch on a laptop or tap with an Android device. The YubiKey was especially beneficial during primary elections when temporary workers had to be hired to manage an influx of mail-in ballots. Every temporary employee received their own security key, which they could use to access the state's voter registration system.

> "Jurisdictions are moving toward implementing multi-factor authentication on their voter registration databases. It's a very cost-effective and easy process and it didn't cost us a lot of money," the state's election director says. "It's such a huge part of making sure systems are secure. I don't see how you can't do it."

> “Government agencies have unique roles in the community, especially during times of crisis when their supply chain infrastructure becomes critical to the community. In many respects, government supply chains need to be more resilient than their commercial counterparts.”
>
> —Deloitte[19]

Supply chain security

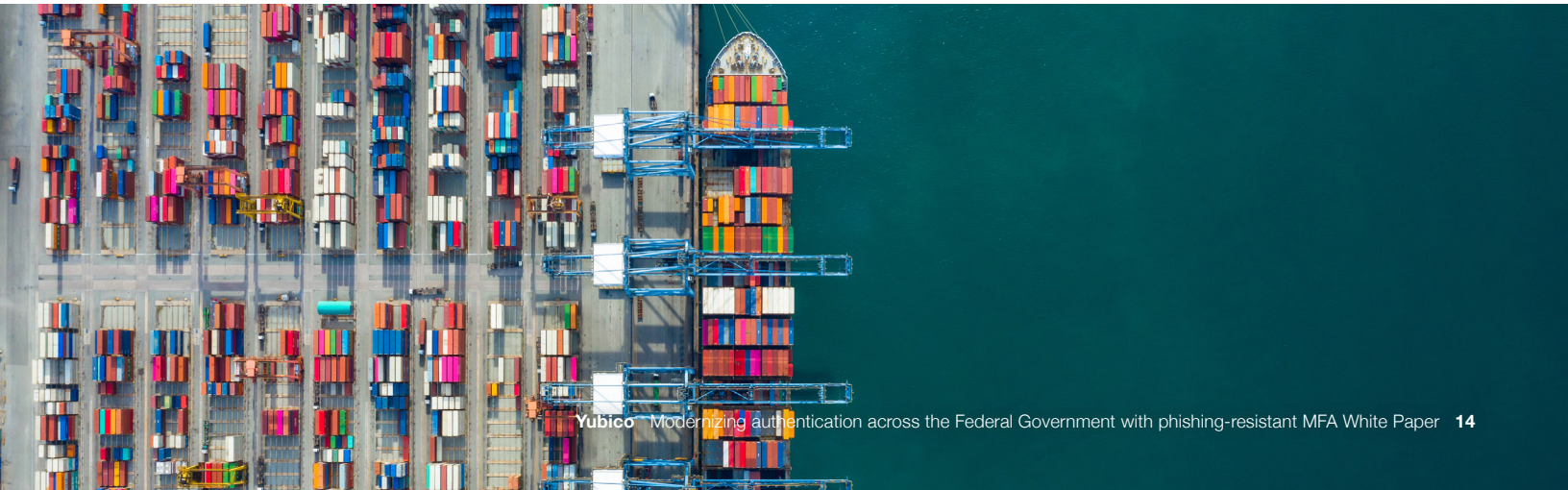
SLTT governments rely heavily on public-private partnerships and a complex supply chain for the products and services (including software) to support its operations. Further, public sector entities are responsible for procurement of critical goods to support public health and safety, including PPE needed in hospitals and by first responders.

The supply chain challenges of the past several years have undermined the importance of building resilience into the supply chain as well as protecting the supply chain against cyberattacks. EO 14028, for example, specifically calls out the lack of transparency and adequate controls to prevent tampering by malicious actors—gaps in the software chain of custody which have been exploited by high profile attacks, including the attack on the Colonial Pipeline oil system in 2021.

SLTT can reduce the risk in the supply chain with the YubiKey for any third-party user who has upstream access to the network and at critical IP handoffs to help ensure all forms of code are protected from unauthorized access and tampering. It is also important to ensure any vendor in the supply chain has proper chain-of-custody and disposal processes for secrets.

Here are a few other questions that would be worth asking a supply chain vendor being considered:

- Do the engineering teams have secure development practices, like training, design reviews and threat modeling?
- Does the vendor’s security team provide automated static and dynamic analysis, performing manual code review and penetration tests for major releases?
- Is there a clear chain of custody of code?
- Are there independent third party reviews of the vendor’s security system and code?
- Is there an incident response team that will be ready to provide speedy security advisories on the day they are needed?
- Are phishing-resistant MFA technologies employed internally by the vendor?
- How is customer data protected and disposed of?
- Is there physical security for the vendor’s servers and infrastructure?
- Are products certified by recognized certification agencies?
- Can the vendor meet your delivery and capacity requirements?



> “Meeting this requirement for the general public will mean providing support for Web Authentication-based approaches, such as security keys.”
>
> —OMB M-22-09[21]

Citizen-facing digital services

External constituents need to seamlessly access citizen services without leaving open attack vectors and creating liability issues. Federal agencies have already been tasked, under OMB M-22-09, to provide public-facing services to provide citizens with “tools they can use to protect themselves” with more authentication tools, including the option to use phishing-resistant MFA.[20]

SLTT governments can build phishing-resistant authentication using FIDO2/WebAuthn and YubiKeys into citizen-facing digital services to help protect against cyberattacks and bridge the divide for those constituents that don’t have or cannot afford a mobile device.

Yubico offers simple procurement and distribution at scale

Yubico offers flexible and cost-effective enterprise plans that help organizations with 500 users or more move away from legacy and broken MFA and accelerate towards phishing-resistant authentication at scale. With YubiEnterprise Subscription, organizations can benefit from a predictable OPEX model, the flexibility to meet user preferences with choice of any YubiKey, upgrades to the latest YubiKeys, and faster rollouts with easy access to Deployment Services, Priority Support and a dedicated Customer Success Manager.

Subscription customers are also eligible to purchase additional services and product offerings, such as YubiEnterprise Delivery, a global turnkey hardware key distribution service to residential and office locations to get YubiKeys directly into the hands of your users.

Grant funding available to SLTT governments to reduce cyber risk

In a Bipartisan Infrastructure Law, Congress established a State and Local Cybersecurity Grant Program (SLCGP) that would make more than $1 billion available over the next four years to help SLTT governments manage and reduce systemic cyber risk.[22] At least 80% of grant funds received by states will be passed on to local governments.

The Cybersecurity and Infrastructure Security Agency (CISA) established objectives for the program, including the need to develop and establish governance structures, to identify areas for improvement in cybersecurity posture, to implement security protections, and to ensure personnel are appropriately trained in cybersecurity.

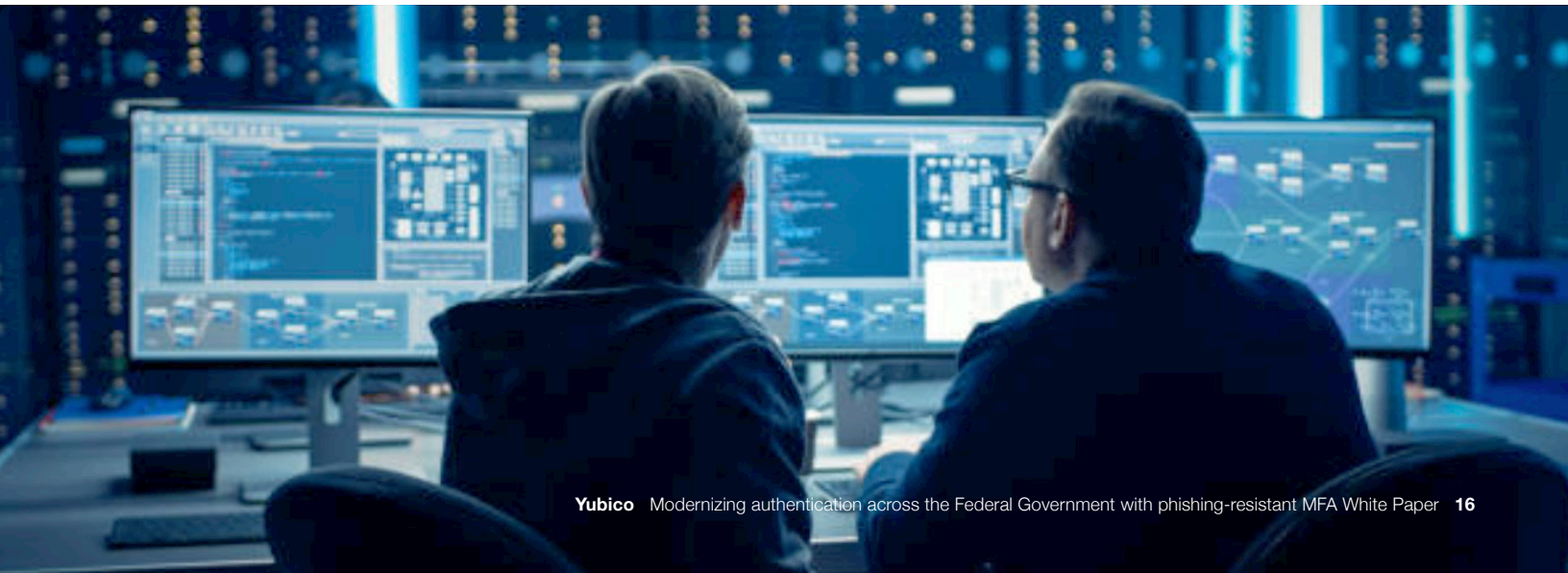
MFA is a part of the CISA's Identity Pillar and will be reviewed as a priority for these grants as part of the required mitigation efforts and several objectives laid out in Appendix C: Cybersecurity Plan of the Notice of Funding Opportunity.

The YubiKey satisfies cybersecurity required elements around:

- **Element 3**: Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- **Element 4**: Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- **Element 5**: Ensure organizations use best practices to enhance cybersecurity, including MFA.

The state's Cybersecurity Plan should highlight the jurisdiction's need for MFA, citing objective three and the above required elements.

An updated total of $200 million was allocated for FY 2022, of which $185 million was allocated to the SLCGP and $6 million under the Tribal Cybersecurity Grant Program (TCGP). Congress authorized the appropriation of $400 million for FY 2023, $300 million for FY 2024 and $100 million for FY 2025. States and territories can begin the application process at any time through the Federal Emergency Management Agency (FEMA).



Takeaway

To protect against the growing number of cyber threats, regulations, and requirements, state, local, tribal and territorial governments need a modern solution to provide phishing-resistant MFA and passwordless authentication at scale and across a wide variety of complex authentication scenarios.

The YubiKey satisfies SLCGP grant requirements and is uniquely designed to help state and local government agencies achieve 100% MFA no matter what stage they are at in their security readiness, meeting stringent cybers insurance security requirements and ensuring compliance with evolving regulations and protecting accounts for employees and constituents, including remote and hybrid workers and privileged users.

Sources

1. US Census, Census of Governments, (February 3, 2021)
2. IBM, Cost of Data Breach Report 2022, (July 27, 2022)
3. Lily Hay Newman, Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare, (April 23, 2018)
4. Paul Bischoff, Ransomware attacks on US government organizations cost $18.9bn in 2020, (March 17, 2021)
5. Jenni Bergal, Florida Hack Exposes Danger to Water Systems, (March 20, 2021)
6. FBI Cyber Division, Private Industry Notification 20220330-001, (March 30, 2022)
7. Deloitte-NASCIO, 2022 Deloitte-NASCIO Cybersecurity Study, (Accessed November 3, 2022)
8. Donald F. Norris, et. al., Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity, (February 21, 2019) available at Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity
9. Lookout, Rise in Mobile Phishing Credential Theft Targeting U.S. Public Sector, (Accessed November 4, 2022)
10. DHS, Biden-Harris Administration Announces $1 Billion in Funding for First-Ever State and Local Cybersecurity Grant Program, (September 16, 2022)
11. Deloitte-NASCIO, 2022 Deloitte-NASCIO Cybersecurity Study, (Accessed November 3, 2022)
12. The White House, Executive order on Improving the Nation's Cybersecurity, (May 12, 2021)
13. Shalanda D. Young, Office of Management and Budget, M-22-09, (January 26, 2022)
14. US Government Information, S.2520
15. Government Finance Officers Association, Cyber Risk Savvy, (2022)
16. Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019)
17. Andras Cser, et. al., The Forrester Wave: Privileged Identity Management, Q4 2018, (November 2018)
18. Derek B. Johnson, Nonprofit rolls out discounted cyber support for political campaigns, (October 31, 2019)
19. Deloitte, Building a more resilient government supply chain, (accessed November 7, 2022)
20. Shalanda D. Young, Office of Management and Budget, M-22-09, (January 26, 2022)
21. Shalanda D. Young, Office of Management and Budget, M-22-09, (January 26, 2022)
22. CISA, State and Local Cybersecurity Grant Program, (Accessed November 2, 2022)

yubico

About Yubico

As the inventor of the YubiKey, Yubico makes secure login easy and available for everyone. The company has been a leader in setting global standards for secure access to computers, mobile devices, and more. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services.

Yubico is privately held, with a presence around the globe. For more information, please visit: www.yubico.com.