Protecting Critical Government Assets with Hardware Security Key-Based Authentication

How do state and local governments typically authenticate users?
For years, state and local governments have relied on usernames and passwords to authentic users. But username and password-based authentication is not good enough anymore. Governments need to improve cybersecurity to protect their constituents against the havoc wreaked by cyberattacks.

To improve authentication security, some state and local government departments have turned to mobile-based MFA.

What are the risks to government when relying on mobile-based MFA?
Mobile authentication may appear to be a quick fix to tighten government security, but it will only protect enterprises up to 80 or 90 percent, leaving critical gaps in coverage. Systems are still vulnerable because governments are relying on downloaded software.

There will also always be employees who either can’t, don’t or won’t use mobile-based MFA. Some employees do not have access to a smartphone or have limited access to Wi-Fi. Others might work for unions that say they cannot use their personal devices for work purposes.

How can a hardware security key help address some of these issues, and provide an alternative or complement to mobile-based MFA?
A mobile authenticator might be easy to distribute, but a hardware security key offers far better security and user experience in the long run. With mobile authentication, every time you want to log in to a system you have to enter your username and password, wait for a code and enter in the code before you start. With a key, you simply enter your username and password, insert your key and you are in.

A hardware security key, such as the YubiKey from Yubico, is phishing resistant. Even if a hacker gets your username and password, if they do not have the key, they cannot infiltrate your system. YubiKeys are also 1 of 3 government-approved alternate authenticators, according to the Department of Defense, and are referenced in the NSA’s guidance on selecting secure MFA solutions. As the keys are also FIPS validated, government customers can quickly fill security gaps with fast deployments and quick budget approvals.

Hardware keys also guarantee a secure supply chain. When your key needs to be updated, you do not have to download new software that could put you at risk. You simply receive a new key.

What should state and local governments be looking for when procuring a hardware security key?
When adopting a new tool or solution, governments should always follow the “crawl, walk, run” model. First, governments should consider how they are currently operating. Then, they need to discuss the quickest way to transition their authentication strategy to a zero trust model that ensures only the right assets are connecting to their network.

For some state and local governments, this might involve first procuring hardware security keys for staff that can’t, don’t or won’t use MFA as a way to fill gaps in coverage.

The ideal hardware security key collaborates with a secure identity platform to create a single sign-on experience for each user. The identity platform automates the process so governments simply can set it and forget it.

Governments already protect the health and public safety of citizens. Cybersecurity is the next domain, and a hardware security key is an easy solution that governments can implement to protect their employees and their constituents from cyberattacks.