The White House's National Cybersecurity Strategy and Pandemic Anti-Fraud Proposal: Three things you should do to respond now

David Treece
March 16, 2023 4 minute read

On March 2, the White House made a clear and important announcement to the tech sector regarding cybersecurity efforts moving forward: "*We must rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, and local governments, and onto the organizations that are most capable and best-positioned to reduce risks for all of us.*"

The White House's announcement outlined a new vision for the administration's new National Cybersecurity Strategy, as well as a sweeping plan to take on fraud in a Pandemic Anti-Fraud Proposal which proposes billions of dollars be invested to combat fraud and identity theft. These announcements build on the administration's May 2021 executive order which put agencies and any company working with the government on notice that MFA would have to quickly become standard practice.

This guidance makes a lot of sense, but shifting the responsibility will also mean these organizations will be liable for poor security deployments that can have legal and financial cost. It remains to be seen what shape the new regulations will take and what financial resources will be put toward all of these efforts, but there's an unmistakable focus and direction to the administration's strategy.

While companies may have had legal leeway in the past about who was responsible for best practices in security and authentication, it's clear that liability is shifting. Starting now, service providers, security firms, software and hardware manufacturers need to design security measures into their solutions, including making strong MFA and passwordless solutions a standard offering – or be faced with future government orders to comply or be fined.

In a recent press briefing following the White House announcement, Acting National Cyber Director Kemba Walden stated it clearly: "*The president's strategy fundamentally reimagines America's cyber social contract. It will rebalance the responsibility for managing cyber risk onto those who are most able to bear it.*"

This announcement comes after several agencies, city and state governments have been hit hard by phishing and ransomware attacks – including a recent damaging attack on the city of Oakland, California. Most of these were a result of successful phishing attempts on legacy MFA or password-based systems that haven't been updated in decades.

What can be done to prepare your company for the regulations to come?

To start, choose a cloud provider and identity access management (IAM) provider that takes security seriously by providing PIV or WebAuthn/FIDO-compliant multi-factor authentication (MFA) options – including security keys like the YubiKey. PIV and FIDO are the gold standards for companies that want high assurance that their end users are who they say they are.

Once that's in place, do these checks on your own security stance:

Are you starting with a zero trust framework?

In other words, are you verifying all users of the system, inside and outside, starting from a foundation that no one is trusted? Beginning with this more holistic approach to security will put you in a better position once the government releases specifics about minimum standards and best practices.

Do you have a code-signing system where every person on your development team is verified and logged each time they take an action?

Even companies whose business is not software developments often have code development teams working on specific applications for internal capabilities. But code management can be vulnerable to phishing attacks and stolen credentials can be used to embed back doors. Code-signing is a best practice today and is likely to be more emphasized in the government's regulatory requirements, so installing a system ahead of time means you'll be prepared.

Do you have a phishing-resistant passwordless authentication system, or are you planning on rolling one out in the next two years?

While the whole world is moving away from a password-based authentication system, it's doing it very slowly because it's still an embedded part of our online culture. But now that FIDO Passkeys and enhancements to PIV deployments are being released through major device suppliers like Apple and Microsoft, passwordless systems are going to be a must-have when the government hands down recommended standards.

This is only the first installment in a series of guidance articles Yubico will be publishing on how to best position your company for the White House's new cybersecurity strategy. Stay tuned to this space as

things develop!

— — —

To learn more about how the YubiKey can be fully integrated into a zero trust architecture, read our whitepaper, Modern Authentication for the Federal Government. To find out which YubiKeys are right for you and your business, try out our quiz here.