ALSTON & BIRD

WWW.ALSTON.COM

Intellectual Property ADVISORY ■

MARCH 13, 2023

New National Cybersecurity Strategy Seeks to Hold Technology Companies Accountable

On March 2, 2023, the Biden Administration released the National Cybersecurity Strategy. Setting the Administration's comprehensive cybersecurity policy, the Strategy seeks to implement several measures to build a "defensible, resilient digital ecosystem" for the United States and its allies. Notably, many of the Strategy's objectives impact technology companies—the Strategy seeks to impose liability on technology companies that fail to take "reasonable precautions to secure their software."

For an overall review of the framework provided by the Strategy, please see our Privacy, Cyber & Data Strategy advisory "White House Releases National Cybersecurity Strategy."

Immediate Impact on Businesses

The Strategy has no immediate impact on the technology industry, although it clearly signals the Administration's directive to aggressively regulate software makers' security practices. The Strategy, by itself, creates no new obligations and has no legal effect. Instead, the Office of the National Cyber Director (ONCD), an executive agency responsible for advising the President on cybersecurity issues, will lead the development of a plan setting out the "Federal lines of effort" necessary to implement the Strategy. Businesses can look to the Strategy as a roadmap for potential legislation and regulation to come, while keeping in mind the actual implementation may substantially differ from what the Strategy outlines.

Notable Issues for Software Companies

The Strategy proposes several cybersecurity measures, but two issues are of particular importance to the technology industry.

National cybersecurity requirements

One of the Strategy's central objectives is the establishment of national cybersecurity requirements. The Administration identifies imposing security obligations on organizations that hold personal data as one of the "fundamental shifts"

required to create a more secure cyberspace. To this end, the Administration specifically calls for federal legislation that will regulate businesses' ability to collect, maintain, and use personal data. Under the Strategy, the Administration will push such legislation to include national security requirements that conform to the standards and guidelines that the National Institute of Standards and Technology (NIST) has developed.

Imposing liability on technology companies

Under the Strategy, the Administration will also "work with Congress and the private sector to develop legislation establishing liability for software products and services." From the Administration's view, the market is incentivizing creation of vulnerable products because the current regulatory landscape lacks strong penalties for technology companies that ignore security best practices. The Strategy calls for federal legislation that imposes liability on businesses that "fail to take reasonable precautions to secure their software." This likely covers companies that physically distribute software, host their software, or distribute physical products with embedded software.

The Strategy suggests what these reasonable precautions should include. First, companies should implement secure-by-default configuration and remove any known vulnerabilities before their products enter the market. Second, companies should conduct thorough due diligence of any third-party components they integrate into their products or face liability from issues caused by such components. Third, companies should follow industry best practices for secure development, including performance of pre-release testing.

Additionally, the Strategy seeks to limit software makers' ability to contractually disclaim their security liabilities. The Administration explains that certain technology companies leverage their superior market positions to fully disclaim their security liabilities when contracting with end users, including consumers and small- to medium-sized businesses. Based on this "market position" statement, the Strategy's aggressive measures appear to mainly target (1) "big tech" companies and other businesses with strong market shares; and (2) makers of consumer-facing software products.

Likely Industry Pushback

We anticipate significant pushback from the industry.

Cybersecurity harms caused by multiple factors

First, it is unclear how the Strategy addresses cybersecurity harms caused by multiple factors from a liability perspective. In today's environment, it is often hard to find a single point of failure that causes security issues. A user often operates an interconnected system of software products, which may create a security risk only in combination. Threat actors may use vulnerabilities in several different products together for exploitation. Besides due diligence requirements for third-party components, the Strategy does not provide meaningful guidance on how the liabilities will be distributed when there are multiple factors that lead to security failures.

The prevalence of open-source software (OSS) in modern software development will add complexity as technology companies try to meet the diligence requirements in the Strategy. As the Administration recognizes, a single software product often incorporates a number of OSS components, and each OSS is continuously being developed and maintained by multiple contributors. These characteristics of OSS increase the difficulty for technology companies to be certain they have vetted all OSS components integrated into their products. Despite these challenges, the

Strategy suggests that technology companies, and not OSS developers, will be responsible for cybersecurity failures arising from the use of OSS.

User-created cybersecurity issues

Second, even if a single point of failure exists, the Strategy does not explain how user-created issues will be weighed. While the Strategy states that technology companies should set default configurations to be secure, it is unclear what types of liability businesses will face when users cause security issues, either intentionally or unintentionally.

It appears the Administration plans to hold technology companies responsible for user errors to a certain degree. For example, the Strategy emphasizes "[a] single person's momentary lapse in judgment, use of an outdated password, or errant click" should not have significant impact on national cybersecurity. This statement can be concerning for the industry, given that technology companies cannot control all user behavior.

Potential safe harbor program

Businesses may gain more clarity on how the Administration will address these concerns as the ONCD establishes the implementation plan, especially around the safe harbor program proposed in the Strategy. The Strategy acknowledges that no security measures can prevent all vulnerabilities. Accordingly, the Administration is planning to develop an "adaptable safe harbor framework" that takes into account relevant best practices, such as the NIST standards.

Important Open Questions

As the Strategy only provides high-level objectives of the Administration, there are several important open questions.

Interaction with state rules

First, the Strategy does not substantively address how these federal initiatives will interact with existing state laws and regulations. The Strategy's objectives encompass rulemaking and legislation on both federal and state levels, but it is unclear how the Administration plans to handle potentially conflicting requirements.

From a security standpoint, a number of states already require certain cybersecurity measures for covered businesses, with some jurisdictions maintaining their own safe harbor programs. From a contractual liability standpoint, state contract laws generally govern the enforceability of contracts, including limitations on liability provisions. At the moment, the Strategy makes a general reference to "collaboration" between different authorities but does not specify preemption or other mechanisms to streamline differing jurisdictional rules.

Private right of action

Second, it is unclear whether the Administration seeks to provide a private right of action for the anticipated cybersecurity requirements. The Strategy encourages states and other regulators to use their existing enforcement authorities to further the Strategy's objectives. But at the moment, the Strategy does not mention a private right of action even though its existence may substantially affect businesses' exposure.

Final Thoughts

The Strategy signals the Administration's willingness to take aggressive cybersecurity measures against big tech and companies processing consumer data. At the moment, however, the Strategy has no impact on the technology industry. An Administration change can also affect the Strategy's implementation, just as how the Strategy replaces the prior national cybersecurity strategy established by the Trump Administration. We will continue to monitor developments surrounding the Strategy, particularly once the ONCD publishes the implementation plan in the coming months.

You can subscribe to future ***Intellectual Property*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or wish to discuss further, please contact any of the following members of Alston & Bird's Intellectual Property Group.

David C. Keating
+1 404 881 7355
+1 202 239 3921
david.keating@alston.com

David S. Teske
+1 404 881 7935
david.teske@alston.com

George M. Taulbee
+1 704 444 1023
george.taulbee@alston.com

Karen M. Sanzaro
+1 202 239 3719
karen.sanzaro@alston.com

Maki DePalo
+1 404 881 4280
maki.depalo@alston.com

Katherine M. Wallace
+1 404 881 4706
katherine.wallace@alston.com

Adria C. Moshe
+1 404 881 7805
adria.moshe@alston.com

Hyun Jai Oh
+1 404 881 7886
hyunjai.oh@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ +1 404 881 7000 ■ Fax: +1 404 881 7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ +1 704 444 1000 ■ Fax: +1 704 444 1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ +1 214 922 3400 ■ Fax: +1 214 922 3899
FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ +1 214 922 3400 ■ Fax: +1 214 922 3899
LONDON: 4th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44 0 20 3823 2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ +1 213 576 1000 ■ Fax: +1 213 576 1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ +1 212 210 9400 ■ Fax: +1 212 210 9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ +1 919 862 2200 ■ Fax: +1 919 862 2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ +1 415 243 1000 ■ Fax: +1 415 243 1001
SILICON VALLEY: 755 Page Mill Road ■ Building C - Suite 200 ■ Palo Alto, California, USA 94304 ■ +1 650 838 2000 ■ Fax: +1 650 838 2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ +1 202 239 3300 ■ Fax: +1 202 239 3333