SIDLEY

Biden Administration Announces National Cybersecurity Strategy

MARCH 29, 2023

CYBERSECURITY, NATIONAL SECURITY, POLICY

Read Time: 4 mins

On March 1, 2023, the Biden administration announced its long-awaited National Cybersecurity Strategy. The strategy is part of the administration's efforts to bolster and modernize public and private responses to cybersecurity threats.

The strategy presents its goals through five pillars:

1. Defend Critical Infrastructure
2. Disrupt and Dismantle Threat Actors
3. Shape Market Forces to Drive Security and Resilience
4. Invest in a Resilient Future
5. Forge International Partnerships to Pursue Shared Goals

To effectuate these goals, the strategy proposes two fundamental shifts in present cybersecurity policy: (1) rebalancing the risks of cybersecurity threats toward industry and the government rather than end users and (2) realigning incentives to promote long-term investments in resilient, defensible systems.

We provide a summary of the strategy further below but highlight here several key components of the strategy.

First, most of the strategy builds on existing priorities, including incident reporting for critical infrastructure, disrupting ransomware groups and other threat actors, leveraging federal procurement regulations to impose cybersecurity standards, and coordinating cross-sectoral cybersecurity issues via the Cybersecurity and Infrastructure Security Agency (CISA).

Second, the Biden administration is seeking to shift the costs of cyber vulnerabilities from consumers to producers and manufacturers. We previously **discussed [https://www.law360.com/articles/1440706]** how this might occur after the President's May 12, 2021 executive order, "Improving the Nation's Cybersecurity." Other administration officials have analogized the effort to placing seatbelts in cars — to shift the burden away from the consumer and onto whichever entity is building the product the consumer uses.

Third, the strategy hints at a few novel proposals that will continue to evolve, such as a federal cyber insurance backstop for certain major cyber events and expanding the ability of the Cyber Safety Review Board to review significant cyber events. The administration also requests additional authorities allowing federal agencies to implement cybersecurity requirements.

Fourth, the administration acknowledges that several of its proposals, such as shifting liability to the producers of software products and services, require legislative action. To this end the strategy reflects the administration's intentions to push for such laws to be created and passed.

While expansive, the publication of the National Cybersecurity Strategy remains a first step. The administration must now implement it — a task that the White House's Office of the National Cyber Director will oversee.

***

Categories

Select Category

Recent Posts

Now You See Them, Now You Don't: Regulatory Risks of Ephemeral Messages
May 1, 2023

New UK Digital Markets Regime: Key Differences With the EU Digital Markets Act
April 27, 2023

The Future of UK Open Banking: Joint Regulatory Oversight Committee Issues Recommendations
April 26, 2023

Compliance Updates for Employer's use of Automated Decisionmaking Tools: New York City Finalizes Rules on Automated Employment Decision Tools and Sets Enforcement Date for July 5, 2023, Upcoming California Regulations, and Federal Guidance
April 24, 2023

FemTech Has Been Warned: UK's ICO Indicates Closer Scrutinization of FemTech Apps
April 20, 2023

Contacts

Kwaku A. Akowuah
Washington, D.C.
+1 202 736 8739
kakowuah@sidley.com

Sheila A.G. Armbrust
San Francisco
+1 415 772 7430
sarmbrust@sidley.com

Francesca Blythe
London
+44 20 7360 2058
fblythe@sidley.com

Colleen Theresa Brown
Washington, D.C.

Summary of Strategy Components

Defend Critical Infrastructure

- Enact performance-based regulations and guidance to requiring compliance with industry best practices as well as incident reports from critical infrastructure and their service providers.
- Increase collaboration among the CISA, federal agencies responsible for specific critical sectors, and individual owners and operators of critical infrastructure.
- Consolidate the federal government's distinct cyber capabilities to create Federal Cybersecurity Centers that can enable a holistic response.
- Establish a "call to one is a call to all" policy for incident notification to federal agencies coordinated by CISA. This will also allow federal agencies to understand what resources are available to them after an incident has occurred.
- Modernize federal systems by replacing legacy systems, migrate to cloud-based services, mitigate the risk of software supply chain, and share certain centralized services.

Disrupt and Dismantle Threat Actors

- Update the Department of Defense's cyber strategy to clarify how the department will integrate cyberspace into its defense efforts.
- Expand the National Cyber Investigative Joint Task Force to coordinate joint takedown and disruption campaigns more frequently, quickly, and on a larger scale.
- Encourage the private sector to use a nonprofit organizations for operational collaboration with the federal government (i.e., National Cyber-Forensics and Training Alliance).
- Warn defenders and notify victims earlier when the government has information that an organization is being targeted or is already compromised.
- Review declassification policies to determine whether expanding clearances or access is necessary to provide actionable intelligence to critical infrastructure owners and operators.
- Prioritize and enforce a risk-based approach to prevent exploitation of U.S.-based infrastructure through implementation of Executive Order 13984, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities."
- Disrupt ransomware via encouraging international cooperation, investigating ransomware crimes, and bolstering infrastructure resilience.
- Target illicit cryptocurrency exchanges that may be financing ransomware operations.

Shape Market Forces to Drive Security and Resilience

- Hold accountable companies that fail to protect consumer privacy.
- Support legislation that lays out national requirements on data security consistent with the National Institute of Standards and Technology (NIST).
- Expand Internet of Things device security labels so that consumers can compare products.
- Shift liability of software vulnerabilities onto software producers, with an adaptable framework as a safe harbor (like NIST's Secure Software Development Framework).
- Use federal grants and procurement regulations to require cybersecurity safeguards for applicants.
- Consider a federal cyber insurance backstop for catastrophic cyber incidents.

Invest in a Resilient Future

- Adopt security measures and support nongovernmental standards-developing organizations to mitigate systemic risks.

+1 202 736 8465
ctbrown@sidley.com

John M. Casanova
Singapore
London
+65 6230 3907
jcasanova@sidley.com

Thomas D. Cunningham
Chicago
+1 312 853 7594
tcunningham@sidley.com

Tomoki Ishiara
Tokyo
+81 3 3218 5014
tishiara@sidley.com

Amy P. Lally
Century City
+1 310 595 9662
alally@sidley.com

David C. Lashway
Washington, D.C.
+1 202 736 8059
dlashway@sidley.com

Linh Lieu
Hong Kong
+852 2509 7868
linh.lieu@sidley.com

William RM Long
London
+44 20 7360 2061
wlong@sidley.com

Joan M. Loughnane
New York
+1 212 839 5567
jloughnane@sidley.com

Geeta Malhotra
Chicago
+1 312 853 7683
gmalhotra@sidley.com

Alan Charles Raul
Washington, D.C.
New York
+1 202 736 8477
+1 212 839 5573
araul@sidley.com

Sean Royall
Dallas
Washington, D.C.
+1 214 981 3330
+1 202 736 8254
sroyall@sidley.com

Jennifer B. Seale
Washington, D.C.
+1 202 736 8640
jseale@sidley.com

Yuet Ming Tham
Singapore
Hong Kong
+65 6230 3969
+852 2509 7645
ytham@sidley.com

- Prioritize research and development to proactively prevent and mitigate cybersecurity risks.
- Establish a process to transition the country's cryptographic systems to quantum-resistant cryptography.
- Prioritize the transition of vulnerable public networks and systems to quantum-resistant cryptography-based environments.
- Build cybersecurity defenses proactively as the U.S. expands its clean energy infrastructure.
- Encourage investments in verifiable, consent-based digital identity solutions.
- Implement a national strategy to develop a cyber workforce.

Forge International Partnerships to Pursue Shared Goals

- Build international coalitions to share cyberthreat information, exchange model practices, compare sector-specific expertise, and coordinate incident response policies.
- Strengthen the capacity of like-minded states to secure their own critical infrastructure, share information, and prosecute cybercrimes.
- Expand U.S. abilities to assist U.S. allies that have been affected by cyber incidents, including the ability to rapidly deploy expertise to respond to cyberattacks.
- Work with the United Nations and our partners to reinforce global norms regarding responsible state behavior.
- Secure global supply chains from disruptions and vulnerabilities by increasing U.S. domestic capacity and working with U.S. allies to build transparent and resilient supply chains.

Alan Charles Raul
WASHINGTON, D.C., NEW YORK

araul@sidley.com

Lauren Kitces
WASHINGTON, D.C.

lkitces@sidley.com

Vishnu Tirumala
WASHINGTON, D.C.

vtirumala@sidley.com

John K. Van De Weert
Washington, D.C.
+1 202 736 8094
jvandeweert@sidley.com

Jonathan M. Wilan
Washington, D.C.
+1 202 736 8635
jwilan@sidley.com

John W. Woods Jr.
Washington, D.C.
+1 202 736 8060
jwoods@sidley.com

You Might Also Like

April 2023 April 2023 April 2023

Compliance Updates for Employer's use of Automated Decisionmaking Tools: New York City Finalizes Rules on Automated Employment Decision Tools and Sets Enforcement Date for July 5, 2023, Upcoming California Regulations, and Federal Guidance

Compliance Updates for Employer's use of Automated Decisionmaking Tools: New York City Finalizes Rules on Automated Employment Decision Tools and Sets Enforcement Date for July 5, 2023, Upcoming California Regulations, and Federal Guidance

Employers in New York City may soon be subject to a new law, **Local Law 144**, that regulates employers' use of automated employment decision tools ("AED tools" or "AEDT") – software and other programs used to make decisions about who to hire, who to promote and other employment decisions. Local Law 144, the first of its kind law regulating these AED tools, was originally supposed to go into effect on January 1, 2023; however, because needed regulatory guidance had not been issued, the effective date was repeatedly pushed back and is now set for July 5, 2023. **Final rules were released** on April 6, 2023, so further delays are unlikely. We summarize below the key provisions of Local Law 144 and what employers need to know to prepare.

AI
Employee Privacy
Policy
U.S. State Privacy Laws

U.S. Securities and Exchange Commission Proposes Three Rules Related to Cybersecurity, Reopens Comment for One Rule

U.S. Securities and Exchange Commission Proposes Three Rules Related to Cybersecurity, Reopens Comment for One Rule

On March 15, 2023, the U.S. Securities and Exchange Commission (SEC) proposed three rules related to cybersecurity and the protection of consumer information and reopened the comment period for a proposed cybersecurity rule for investment advisers and funds. This significant action would impose new cybersecurity requirements for several SEC-registered entities, including with respect to these entities' policies, incident response and notification procedures, and cybersecurity risk management. This Sidley commentary and analysis discusses the key features of each proposal, including new requirements and differences among each of the proposals.

Cybersecurity
Regulation
SEC

New U.S. FDA Draft Guidance Outlines Path To Faster Modification of AI/ML-Enabled Devices

New U.S. FDA Draft Guidance Outlines Path To Faster Modification of AI/ML-Enabled Devices

The U.S. Food and Drug Administration (FDA or Agency) has issued new draft guidance on "Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine Learning (AI/ML)-Enabled Device Software Functions"[1] that discusses a "science-based approach to ensuring that AI/ML-enabled devices can be safely, effectively, and rapidly modified, updated, and improved in response to new data."[2] This approach should offer more certainty to industry as FDA's stated goal is to allow AI/ML-enabled devices to be modified faster in accordance with FDA requirements while being "built to adapt to the data and needs of individual health care facilities" and "adapt to deliver treatments according to individual users' particular characteristics and needs."[3] Those wishing to comment on the draft guidance should note that the comment period closes on July 3, 2023.

AI
Cybersecurity
FDA
Health Privacy
Policy

SIDLEY