JENNER & BLOCK

Client Alert: A Cybersecurity Roadmap: The National Cybersecurity Strategy Implementation Plan (July 2023)

Publications

July 19, 2023
By: Shoba Pillay, David Bitkower

On July 13, 2023, the White House published the National Strategy Implementation Plan (the Implementation Plan).[1] According to the White House, the Implementation Plan is a "roadmap to realize" the mission of the National Cybersecurity Strategy (the Strategy), which was released in March.[2]

In a March 9, 2023 client alert, we outlined the Strategy's objectives and anticipated impact, including the five pillars crucial to developing a more secure digital ecosystem: (1) defense of critical infrastructure; (2) disruption of threat actors; (3) use of market forces to incentivize security and resilience; (4) federal investment; and (5) international partnerships.[3] In addition, the Strategy breaks each pillar into several strategic objectives.[4]

The Implementation Plan is one of the first steps in the White House's execution of its Strategy, which will ultimately take years to fully implement. The White House noted that the Implementation Plan is a "living document" and that we can expect annual iterations of the Plan.[5]

I. Implementation

Portions of the Strategy are already in progress. On June 20, 2023, the Department of Justice announced a new National Security Cyber Section in the National Security Division.[6] On June 27, 2023, the Office of Management and Budget (OMB) issued a memorandum that outlines cybersecurity investment priorities for the federal government's fiscal year 2025 budget and guidelines for agencies' budget submissions.[7]

The Implementation Plan assigns each of the Strategy's initiatives to a federal agency and provides ambitious deadlines for the completion of each. Several of the implementation plans will impact the private sector, including:

1. By **early 2024**, the Office of the National Cyber Director must host stakeholders for a legal symposium to explore different approaches to developing the software liability framework laid out in the Strategy—which will involve holding liable software companies that do not follow best cybersecurity practices.[8] The legal symposium will involve discussions with software stakeholders in the private sector to develop a well-informed approach to the liability regime.[9]

2. By the **end of 2024**, the Cybersecurity and Infrastructure Security Agency (CISA) will offer resources to "high-risk targets" of ransomware, including critical infrastructure organizations, to increase their protections against ransomware attacks.[10] Those resources may include "training, cybersecurity services, technical assessments, pre-attack planning, and incident response."[11]

3. By **early 2025**, the National Security Council, in coordination with the Office of the National Cyber Director and Sector Risk Management Agencies, must establish cybersecurity requirements across critical infrastructure sectors.[12] The sixteen critical infrastructure sectors include industries such as communications, critical manufacturing, energy, financial services, food and agriculture, healthcare, information technology, and transportation systems.[13]

4. As we previewed in March, CISA is responsible for issuing a final critical infrastructure cyber incident reporting rule.[14] When the final rule is implemented, it will require covered entities to report covered cyber incidents to CISA within 72 hours of the incident, and ransomware payments within 24 hours of making the payment.[15] According to the Implementation Plan, by **fall of 2025** companies will have clarity about (1) whether they are a covered entity and (2) what types of cyber incidents must be reported to CISA.[16]

II. Opportunities for Clients

Like the Strategy, the Implementation Plan calls for input from the private sector.[17] In particular, the Implementation Plan asks agencies to partner with the private sector to implement the plan.[18] The White House welcomed feedback from the private sector, promising to refine the Implementation Plan in response to private sector assessments of each initiative's effectiveness.[19]

Private sector entities should look for opportunities to assess the effectiveness of implementation efforts and provide the White House with feedback where appropriate. Jenner & Block stands ready to assist clients in making that assessment and in preparing for the implementation of the National Cybersecurity Strategy.

Footnotes

[1] National Cybersecurity Strategy Implementation Plan (July 13, 2023), National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf (whitehouse.gov) (Implementation Plan).

[2] Fact Sheet (July 13, 2023), FACT SHEET: Biden-Harris Administration Publishes the National Cybersecurity Strategy Implementation Plan | The White House.

[3] National Cybersecurity Strategy (March 1, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (Strategy).

[4] Strategy.

[5] Implementation Plan.

[6] https://www.justice.gov/opa/pr/justice-department-announces-new-national-security-cyber-section-within-national-security.

[7] https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-18-Administration-Cybersecurity-Priorities-for-the-FY-2025-Budget-s.pdf.

[8] Strategy at 20; https://www.jenner.com/en/news-insights/publications/client-alert-biden-harris-administration-cybersecurity-strategy.

[9] Implementation Plan at 30.

[10] Implementation Plan at 27.

[11] Implementation Plan at 27.

[12] Implementation Plan at 13.

[13] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

[14] https://www.jenner.com/en/news-insights/publications/client-alert-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022.

[15] https://www.jenner.com/en/news-insights/publications/client-alert-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022.

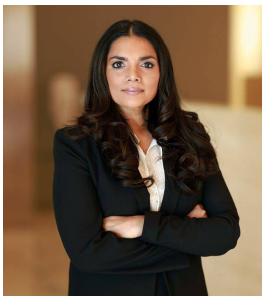
[16] Implementation Plan at 18.

[17] Implementation Plan at 4.

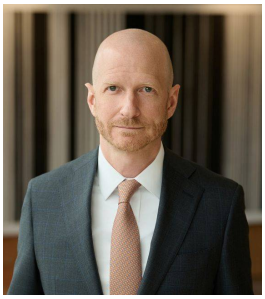
[18] Implementation Plan at 4.

[19] Implementation Plan at 4.

Related Attorneys



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605



David Bitkower
Partner
dbitkower@jenner.com
+1 202 639 6048

Related Capabilities

Data Privacy and Cybersecurity

Stay Informed →