# Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : 01279296 | Mar 15, 2023, 02:36 PM

This week, *Hacking Healthcare* examines the newly published United States National Cybersecurity Strategy. After briefly summarizing the structure and primary engagement areas, we dive into which kinds of impacts the strategy may have on the healthcare sector.

Welcome back to *Hacking Healthcare*.

**U.S. National Cybersecurity Strategy**

The Biden-Harris administration recently released their National Cybersecurity Strategy on March 2, 2023. The new strategy, the first since 2018, builds on President Biden's earlier cybersecurity efforts and is partially shaped by the SolarWinds, Colonial Pipeline, and JBS attacks.[i] While devoid of specific action items, the strategy signals the lines of effort that the administration is prioritizing, and more than a few are expected to have significant impacts on the healthcare sector.

The strategy is based around five key pillars of interest that sets goals for the next decade of investment and cooperation in cyberspace. The strategy is unique in that it seeks to adjust how the government prioritizes and allocates roles, responsibilities, and resources in cyberspace.[ii] While not wholly divergent from previous strategies and existing initiatives, the new national cybersecurity strategy does emphasize two important distinctions.

First, it recognizes the need to shift the burden of cybersecurity responsibility from small businesses and individuals to those who have the resources and capacity to take it on. In this regard, the document states that "our collective cyber resilience cannot rely on the constant vigilance of our smallest organizations and individual citizens."[iii]

Secondly, the strategy also affirms the need to focus on building a digital ecosystem that is "more resilient and defensible over the long term."[iv] The strategy outlines how this shift encompasses adjusting market forces, attending to the workforce shortage, embracing secure by design principles, and promoting strategic coordination. Notably, it states that the federal government's actions will prioritize "minimally invasive actions."[v]

The Administration recognizes that these themes will not be achieved without public-private cooperation and encourages the private sector to assume its share of responsibility alongside the government.

The National Cyber Strategy is broken down into the following five pillars, each with their own strategic objectives:

**Defend Critical Infrastructure**

In order to ensure the safety and security of the nation's critical infrastructure, the Administration sets out goals to establish cybersecurity requirements that directly support national security and public safety. This includes encouraging harmonizing new and existing regulations while enabling regulated entities to afford security. This pillar also highlights scaling public-private collaboration, integrating federal cybersecurity centers, updating federal incident response plans and processes, and modernizing federal defense systems.[vi]

**Disrupt and Dismantle Threat Actors**

This pillar's strategic objectives include integrating the deployment of federal disruption activities and enhancing public-private operational collaboration to disrupt adversaries.[vii] In order to achieve these goals, this pillar notes that increasing the speed and scale of intelligence sharing and victim notification are integral as well as make it easier for victims to report abuse. This pillar is targeted at countering cybercrime with a specific focus on defeating ransomware, which has been the cause of so many recent largescale disruptions.

**Shape Market Forces to Drive Security and Resilience**

In order to address the security and resiliency of America's digital ecosystem, the strategy says it is necessary to hold the "stewards of our data" accountable.[viii] Other strategic objectives within this pillar include securing IoT devices, shifting liability for insecure software products and services, leveraging federal grant money to build secure-by-design, federal procurement to improve accountability, and exploring a federal cyber insurance backstop.

**Invest in a Resilient Future**

Financing and long-term investments are key elements in ensuring the nation's cybersecurity. This pillar's strategic objectives highlight the need to secure the technical foundation of the internet, reinvigorate federal research and development in cybersecurity, and strengthen the cyber workforce. This pillar also specifically addresses supporting a digital identity ecosystem, a clean energy future, and a post-quantum future.

**Forge International Partnerships to Pursue Shared Goals**

In order to counter threats against the digital ecosystem, this pillar seeks to build coalitions with a diverse group of partners around a democratic vision of cyberspace. It desires to strengthen the capacity for international partners, expand the U.S.' ability to assist its allies, reinforce global norms of responsible state behavior, and secure global supply chains for information, operational technology products, and services.[ix]

In terms of implementation, the Office of the National Cyber Director (ONCD) is now tasked with working with the Office of Management and Budget (OMB) to coordinate the implementation of the pillars.

*Action & Analysis*

*Included with Health-ISAC Membership*

***Congress***

Tuesday, March 14th:

- No relevant hearings

Wednesday, March 15th:

- No relevant meetings

Thursday, March 16th:

- Senate – Homeland Security and Governmental Affairs Committee: Hearings to examine the cybersecurity risks to the healthcare sector

***International Hearings/Meetings***

- No relevant meetings

[i] https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/
[ii] https://www.lawfareblog.com/biden-harris-administration-releases-new-national-cybersecurity-strategy#:~:text=The%20new%20cyber%20strategy%20presents,vision%20in%20five%20strategic%20objectives.
[iii] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[iv] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[v] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[vi] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[vii] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[viii] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[ix] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[x] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[xi] https://www.scmagazine.com/feature/device-security/new-fda-authority-for-medical-device-security-signals-big-changes-for-manufacturers
[xii] https://healthitsecurity.com/news/white-house-sets-sights-on-new-healthcare-cybersecurity-standards
[xiii] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[xiv] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

---

**Reference | References**

**Whitehouse**
**SC Magazine**
**weforum**
**Health-ISAC DDoS Whitepaper**
**Lawfare Blog**
**Health IT Security**
**Lawfare Blog**

**Report Source(s)**

**Health-ISAC**

**Tags**

National Cyber Strategy, Legislation, Regulation, Hacking Healthcare

---



**For Questions and/or Comments:**

Please email us at contact@h-isac.org

**Conferences, Webinars, and Summits:**

**https://h-isac.org/events/**

**Hacking Healthcare:**

Written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

**Access the Health-ISAC Intelligence Portal:**

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.