HACKING HEALTHCARE™

Health-ISAC Weekly Blog -- Hacking Healthcare™

TLP:WHITE

Jul 19, 2023

This week, *Hacking Healthcare*™ examines the newly released National Cyber Strategy Implementation Plan. We break down what this document is, analyze and provide background on the specific initiatives most likely to impact the healthcare sector, and suggest opportunities to engage or influence them.

Join us for the Monthly Threat Briefing

But first, as a reminder, next Tuesday is the Health-ISAC's monthly threat briefing. Come join your fellow Health-ISAC members as Health-ISAC staff and partner organizations provide an overview of the threat landscape. Presentations include an assessment of emerging malware, APT trends, legal and regulatory issues, physical security concerns, and more. We encourage all Health-ISAC members to take advantage of this service.

National Cybersecurity Implementation Plan

On July 13, The United States' National Cybersecurity Implementation Plan was publicly released.[i] This 57-page document outlines the roadmap that the U.S. government will pursue to accomplish the various objectives set out by National Cybersecurity Strategy released back in March of this year. Since critical infrastructure protection and the disruption of malicious cyber actors were a major part of the National Cyber Strategy, let's examine some of the initiatives most relevant to healthcare and see how the U.S. government plans to achieve these goals.

As a brief reminder, the 39-page National Cybersecurity Strategy is based around the idea of achieving two significant shifts in the cybersecurity ecosystem. First, it pushed for those entities capable of doing more to bear a larger responsibility for security and resiliency. Second, it acknowledged the need to shift incentive structures towards investing in long-term resilience. Those two high-level objectives flowed down into five key pillars of interest that sets goals for the next decade of investment and cooperation in cyberspace.

The two pillars likely to be the most relevant for the healthcare sector are the need to defend critical infrastructure and the need to disrupt and dismantle malicious cyber threats. The operationalization of these pillars, outlined in the initial strategy, were described only in broad terms and they included notions around harmonizing regulations, improving and expanding public-private collaboration and information sharing, and cracking down on ransomware. However, the specifics around these actions, who would be responsible for them and when they might be expected to be done, were not specified. The newly released implementation plan goes some way towards fleshing those parts out.

Implementation

Running a hefty 57-pages, the National Cybersecurity Strategy Implementation Plan is described by its authors as the roadmap for

implementation of the various efforts described in the National Cybersecurity Strategy.

Readers should be aware that the document does not necessarily outline which initiatives are being more heavily resourced or prioritized, and even at 57-pages and detailing 65 initiatives, it does not fully capture all of the related governmental activities that ultimately are rooted in the strategy. Importantly, its authors note that that this implementation plan is only the first iteration of what will be a routinely updated living document.

Action & Analysis

Included with Health-ISAC Membership

Congress

Tuesday, July 18

No relevant hearings

Wednesday, July 19

No relevant meetings

Thursday, July 20

No relevant meetings

International Hearings/Meetings

No relevant meetings

EU

[i] https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf

[ii] https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf

[iii] https://405d.hhs.gov/post/detail/b8756c82-9cbb-4309-a0d1-eb80be9a1e58

[iv] https://healthsectorcouncil.org/wp-content/uploads/2023/06/Considerations-for-Prioritized-Recognized-Cybersecurity-Practices.pdf

[v] https://www.cisa.gov/securebydesign

[vi] https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf

[vii] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

[viii] https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022

Reference(s)	CISA Alerts, Whitehouse, federalregister, HHS, Health-ISAC , Health Industry Cybersecurity Practices, CISA Alerts

Report Source(s)	Health-ISAC

Alert ID b728fae9

View Alert

Tags Biden, ONCD, National Cyber Strategy, Hacking Healthcare, Information Sharing, Policy

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

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.

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.