October 19, 2022

TLP White

This week, Hacking Healthcare begins with a brief run through of a new guidance document on supply chain security from the UK's National Cyber Security Centre (NCSC) that coincides with an uptick in supply chain attacks. Next, we summarize a significant number of Biden administration cybersecurity efforts that are likely to impact the healthcare and public health (HPH) sector in both the short and long term within the US. This includes comments from the Deputy National Security Advisor, and excerpts from the recently released National Security Strategy and White House fact sheet on cybersecurity which all point to a changing cybersecurity landscape for the HPH sector.

Welcome back to *Hacking Healthcare*.

1. **Health-ISAC Monthly Threat Brief**

   As a reminder, next Tuesday the Health-ISAC will be holding its monthly Threat Brief. This hour-long presentation from the Health-ISAC staff and Health-ISAC partners briefs members on current and emerging technical, physical, legal, and regulatory threats to the HPH sector. The Threat Brief is private and free to Health-ISAC members.

2. **UK NCSC Warns of Increase in Supply Chain Attacks**

   Supply chain attacks have gained prominence recently with malicious cyber actors often finding it easier to reach intended targets through less well defended suppliers. Following a recent spate of supply chain attacks, the UK's NCSC has issued fresh guidance designed primarily for medium and larger organizations to help "assess the cyber risks of working with suppliers and gain assurance that mitigations are in place."[1]

   The freely available 29-page document provides an accessible framework for organizations to follow. Helpfully, the NCSC approach is organized into five stages that includes what to consider before embarking on your journey to assess and mitigate supply chain risk and how to continuously improve after you've implemented your plan. The five stages are:[2]

1. Before you start
2. Developing an approach to assess supply chain cybersecurity
3. Applying the approach to new supplier relationships
4. Integrating the approach to existing supplier relationships
5. Continuously improving

Taken together, these steps combine to help organizations "gain confidence in [their] supply chain cybersecurity.[3]"

The document was written with "procurement specialists, risk managers and cybersecurity professionals wanting to establish (or improve) an approach for assessing the cybersecurity of their organisation's supply chain" in mind, but it can be helpful to anyone looking to understand a fairly strategic and high-level way of implementing a supply chain security strategy.[4]

Action and Analysis
Membership required

3. Biden Administration National Security Strategy and Critical Infrastructure Announcements

Cybersecurity awareness month appears to be living up to its name with the Biden administration making a number of notable announcements that have summarized recent administration cybersecurity efforts, while also outlining where they plan on focusing their energy going forward.

Administration Fact Sheet

On October 11th, the White House published a fact sheet entitled *Biden-Harris Administration Delivers on Strengthening America's Cybersecurity*.[5] Predictably, the administration's first focus is on improving the cybersecurity of critical infrastructure sectors, with healthcare specifically mentioned. Performance-based directives and cybersecurity performance goals were the throughline here, and they were cited as one area that will see continued effort.

Additionally, the fact sheet touched on the Biden administration's increasingly broad international engagement. There appears to be a sustained effort to work with foreign partners to counter malicious cyber threats and support cyber norms, such the avoidance of targeting critical infrastructure.

However, the most notable aspect might be the announcement of an effort to create a cybersecurity labeling scheme for IoT devices. Details are sparse at the time of writing, but this initial labeling effort does not seem to extend to medical devices.

Critical Infrastructure Focus Expands

While the energy and transportation sectors have seen a bit more tailored focus in recent months, it appears those efforts are broadening to a wider range of critical infrastructure sectors. Speaking at an event last week, the Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, Anne Neuberger, announced that healthcare, water, and communications were set to receive increased attention. While specific details were not forthcoming, she is quoted as saying that Health and Human Services (HHS) will be "beginning work with partners at hospitals to put in place minimum cybersecurity guidelines, and then further work upcoming thereafter on devices and broader healthcare as well."[6]

Commented [JB1]: Is this correct?

Commented [MTC2R1]: Fixed.

National Security Strategy

Finally, the Biden administration also released an updated National Security Strategy.[7] The National Security Strategy is a document that outlines the issue areas that are of particular concern from a national security perspective and then briefly describes how the administration is or is planning to address them. Cybersecurity issues have increasingly been cited in recent years and this most recent strategy document was no exception.

The document calls out the threat of cyberattacks on national health systems and the importance of improving the security and resiliency of critical infrastructure sectors from cyber threats. Included in this was the reiteration that they "are working closely with allies and partners, such as the Quad, to define standards for critical infrastructure to rapidly improve our cyber resilience."[8]

Additionally, the document suggested that the administration may be more aggressive and proactive in responding to cyber threats by saying "We aim to deter cyberattacks from state and non-state actors and will respond decisively with all appropriate tools of national power to hostile acts in cyberspace, including those that disrupt or degrade vital national functions or critical infrastructure."[9]

Action and Analysis
Membership required

Congress

Tuesday, October 18th:
- No relevant hearings

Wednesday, October 19th:
- No relevant hearings

Thursday, October 20th:
- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

Conferences, Webinars, and Summits

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

Contact us: follow @HealthISAC, and email at contact@h-isac.org

About the Author

Hacking Healthcare is 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.

---

[1] https://www.ncsc.gov.uk/news/ncsc-issues-fresh-guidance-following-recent-rise-in-supply-chain-cyber-attacks
[2] https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security
[3] https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security/executive-summary
[4] https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security
[5] https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/
[6] https://www.meritalk.com/articles/white-house-eyeing-cyber-work-on-comms-water-healthcare-sectors/
[7] https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[8] https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf
[9] https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf