Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ **TLP:WHITE** **Alert Id: 8e4e050d** **2024-06-27 18:06:27**

This week, *Hacking Healthcare*™ follows up on our previous examination of the Biden administration's National Security Memorandum 22 (NSM-22). Specifically, we take a look at a recent memo published by the Secretary of the Department of Homeland Security (DHS) providing strategic guidance for, and a prioritization of, critical infrastructure security and resiliency.

Welcome back to *Hacking Healthcare*™.

DHS Releases Memo Outlining National Priorities for Critical Infrastructure Security and Resiliency

A little over a month ago, *Hacking Healthcare* covered the Biden administration's publication of NSM-22.[i] That memorandum revised the U.S. approach to protecting critical infrastructure and clarified the roles and responsibilities of government entities toward implementing the new policy. Recently, DHS Secretary Alejandro Mayorkas released a follow-up memo to NSM-22, *Strategic Guidance and National Priorities for U.S. Critical Infrastructure Security and Resilience,* that outlines more specifically the priorities of DHS and the Cybersecurity and Infrastructure Security Agency (CISA) regarding operationalizing elements of NSM-22.[ii] Let's examine what it says and how it may affect the healthcare and public health (HPH) sector.

Content: Cyber-Related Priority Risk Areas

The memo cites five specific priority risk areas that need to be addressed. While the memo remains consistent with NSM-22's "all threats and hazards" approach, tellingly, four of the five risk areas are closely or directly related to cybersecurity and cyber resiliency, reinforcing just how critical DHS views cyber threats. The four cyber-related priority risk areas are:

PRC Cyber Threats: The memo cites the People's Republic of China's (PRC) "capability to launch cyberattacks on U.S. critical infrastructure and its willingness to target defense critical infrastructure (DCI) and other key critical infrastructure systems and assets to achieve its long-term strategic objectives."[iii][RFE1]

Emerging Technologies: It is unsurprising that artificial intelligence (AI), quantum computing, and other emerging technologies are also cited as priority risk areas. In particular, while acknowledging the "transformative" capacity of AI and its potential to integrate into security tools, the memo cites the need to consider the implications these technologies may have on critical infrastructure sectors.

Critical Infrastructure Dependencies on Space Systems and Assets: The memo notes that "[t]echnology has advanced to the point that access to space-based services, like the Global Positioning System (GPS) and satellite communications, is taken for granted across critical infrastructure."[iv] An example provided was the Russian cyberattacks against commercial satellite communications in support of Russia's invasion of Ukraine.

Supply Chain Vulnerabilities: Healthcare is prominently on display here as the memo leans into the supply chain disruptions caused by COVID-19 and highlights how "offshoring significant parts of critical supply chains and the need to reemphasize resilience alongside efficiency as part of the preparation for future public health and other crises."[v] While those elements lean more toward physical supply chains, the memo does also reference the role of essential services necessary for critical infrastructure operations.

These four are also joined by an acknowledgment of climate change as a factor that could cause additional risk.

Content: Cyber-Related Priority Mitigations

In addition to highlighting priority risks, the memo also outlined priority risk mitigations. All of these mitigations have a cyber component.

Resilience and Recovery: Described within an "all threats and hazards" context, the memo accepts that making critical infrastructure "impervious" to all threats and hazards, including cyber incidents like

ransomware, is impossible. The memo reiterates that the focus must be on building up resilience and the ability to recover from setbacks quickly.

Security and Resiliency Baselines: In alignment with what HHS and Deputy National Security Advisor Anne Neuberger have been warning was coming, the memo underscores the need to develop and implement mandatory security and resiliency requirements for critical infrastructure sectors.

Service Providers: The memo notes that "increasingly, critical infrastructure owners and operators are dependent on the providers of shared infrastructure, products, or services."[vi] While these can provide obvious benefits around efficiency and cost, they can introduce concentration risk.[vii] The memo calls for DHS to work with critical infrastructure vendors and providers of shared services to ensure these services are secure.

Concentrated Risk and Systemically Important Entities: Secretary Mayorkas reiterated the ongoing work to "identify sector, cross-sector, and nationally significant risk" and the need "to identify and prioritize systemically important entities."[viii] Here again, healthcare was put in the spotlight as the memo highlights that, as a "recent ransomware attack on a major health insurer demonstrated, there can also be previously unknown or underappreciated concentration of risks within a particular sector."[ix]

National Coordinator Actions

The memo concludes with a brief paragraph explaining how the National Coordinator, as outlined in NSM-22, will take the lead to drive efforts related to the above priorities and will ultimately address them in a forthcoming National Infrastructure Risk Management Plan.

Let's analyze these issues a bit deeper in the Action & Analysis section.

Action & Analysis

Included with Health-ISAC Membership

[i] https://h-isac.org/health-isac-hacking-healthcare-5-9-2024/

[ii]https://www.dhs.gov/sites/default/files/2024-06/24_0620_sec_2024-strategic-guidance-national-priorities-u-s-crit

[iii]https://www.dhs.gov/sites/default/files/2024-06/24_0620_sec_2024-strategic-guidance-national-priorities-u-s-crit

[iv]https://www.dhs.gov/sites/default/files/2024-06/24_0620_sec_2024-strategic-guidance-national-priorities-u-s-crit

[v]https://www.dhs.gov/sites/default/files/2024-06/24_0620_sec_2024-strategic-guidance-national-priorities-u-s-crit

[vi]https://www.dhs.gov/sites/default/files/2024-06/24_0620_sec_2024-strategic-guidance-national-priorities-u-s-crit

[vii] For those looking to learn more about concentration risk, the following report on Concentration Risk in Federal IT helps outline the issue:
https://www.centerforcybersecuritypolicy.org/insights-and-research/addressing-concentration-risk-in-federal-it

[viii]https://www.dhs.gov/sites/default/files/2024-06/24_0620_sec_2024-strategic-guidance-national-priorities-u-s-cr

[ix]https://www.dhs.gov/sites/default/files/2024-06/24_0620_sec_2024-strategic-guidance-national-priorities-u-s-crit

[x] https://hphcyber.hhs.gov/performance-goals.html

[xi] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

[xii] https://www.hhs.gov/sites/default/files/fy-2025-budget-in-brief.pdf

[xiii]https://www.semafor.com/article/06/18/2024/white-house-eyes-cybersecurity-rule-for-hospitals-in-next-few-wee

Reference(s): semafor, HHS, HHS, CISA , DHS, Health-ISAC , centerforcybersecuritypolicy

Report Source(s): Health-ISAC

Tags: Elections, NSM-22, CPGs, Resiliency, Hacking Healthcare, DHS, Policy

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

Conferences, Webinars, and Summits:

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

Hacking Healthcare■:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has 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.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC■s annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC■s monthly Threat Briefing.

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

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

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.

For Questions or Comments:

Please email us at toc@h-isac.org