Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ ○ TLP:WHITE Alert ID : 41b55355 Mar 18, 2024, 10:50 AM

This week, *Hacking Healthcare*TM examines President Biden's proposed U.S. federal budget for fiscal year 2025 (FY 2025). After a quick primer on what this budget is, we highlight some of the significant cybersecurity takeaways for entities like the Department of Health and Human Services (HHS) and the Food and Drug Administration (FDA). Finally, we wrap up with some analysis of major themes in the budget and what to expect next.

Welcome back to *Hacking Healthcare*TM.

Healthcare Cybersecurity Takeaways from President Biden's FY 2025 Budget

What Is This Budget?

On March 11, President Biden released his proposed budget for FY 2025. The FY 2025 budget outlines President Biden's vision for determining how departments and agencies should be allocated funding by Congress to carry out their respective missions and achieve identified policy goals. This information helps identify the president's priorities and signals both general and specific policy intent.

Beyond various White House-released Fact Sheets and the 188-page Budget of the U.S. Government: Fiscal Year 2025 Document are summary tables, appendices, analytical perspectives, and individual department and agency budget justifications that total thousands of pages.[i], [ii]

For our purposes, we have focused on reviewing the cybersecurity elements of HHS and FDA to identify takeaways that could impact Health-ISAC members.

Key Points: HHS

Within the various HHS-related FY 2025 documents there are several key points worth highlighting. These points include:[iii], [iv], [v], [vi]

HHS

- **Hospital Cybersecurity Standards:** Noting the potential lack of incentives for hospitals to prioritize cybersecurity efforts, HHS laid out a proposal that would "encourage hospitals to upgrade their cybersecurity practices." This proposal, which amounts to requiring minimum cybersecurity standards, includes the following elements:
    1. Increasing cybersecurity expectations over time, beginning with the implementation of "essential" practices, and ending with "enhanced" practices
    2. Investing $800 million from the "Medicare Hospital Insurance Trust Fund over FY 2027 and FY 2028 to approximately 2,000 high-needs hospitals"
    3. Investing $500 million from the Medicare Hospital Insurance Trust Fund for all hospitals to implement enhanced cybersecurity practices in FY 2029 and 2030
    4. Implementing new financial penalties within the "Promoting interoperability program as specific consequences of failing to adopt essential cybersecurity practices," beginning in FY 2029.
    5. Centers for Medicare and Medicaid Services (CMS) could add enhanced cybersecurity practices to its list of required cybersecurity practices beginning in FY 2031

- **Critical Infrastructure Protection (CIP) program:** A proposed increase of $12 million to "support [the Administration for Strategic Preparedness and Response (ASPR)] –CIP program, which will improve HHS-wide coordination and response to cyber incidents affecting the Healthcare and Public Health Sector." ASPR has identified that the additional funding would support:
    1. The execution of HHS' Cybersecurity Strategy, as outlined in last December's Healthcare Sector Cybersecurity Concept Paper[vii]
    2. The implementation of the Healthcare and Public Health (HPH) Cybersecurity Performance Goals through educational campaigns, implementation guidance, technical assistance, and resource development
    3. Increasing "cybersecurity operations to analyze cyber-attack information, assist HPH cyberattack victims, share intelligence with partners, and inform sector partners of risks and mitigations"

FDA

- **Legislative Proposal: Medical Device Shortage Authority Revision:** The FDA identified that new authorities it received during the COVID-19 public health emergency (PHE), which allowed it greater visibility into potential and actual medical device shortages, should be revised to remove restrictions that they must be used in relation to a PHE. Noting that shortages of medical devices can occur from a variety of circumstances, including cybersecurity incidents, the FDA would like Congress to:

1. Update Section 506J of the Federal Food, Drug, and Cosmetic Act (FD&C Act) to remove the temporal limitation "that only requires manufacturers to notify FDA about interruptions or discontinuances in the manufacture of certain devices during or in advance of a PHE"
2. Provide FDA the authority to review risk management plans to "help ensure manufacturers have plans in place to build resiliency and mitigate future supply chain disruptions"

Action & Analysis

Included with Health-ISAC Membership

Upcoming International Hearings/Meetings

EU

- No relevant meetings at this time

US

- No relevant meetings at this time

Rest of World

- Health-ISAC APAC Summit (3/19 - 3/21)

[i] https://www.whitehouse.gov/wp-content/uploads/2024/03/budget_fy2025.pdf

[ii] https://www.whitehouse.gov/omb/briefing-room/2024/03/11/fact-sheet-the-presidents-budget-for-fiscal-year-2025/

[iii] https://www.hhs.gov/about/budget/fy2025/index.html#bib

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

[v] https://aspr.hhs.gov/AboutASPR/BudgetandFunding/Documents/FY2025/ASPR-cj.pdf

[vi] https://www.fda.gov/media/176925/download?attachment

[vii] https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf

Report Source(s)

Health-ISAC

Release Date

Mar 18, 2024, 11:59 PM

Tags

Critical Infrastructure Protection program, Hacking Healthcare, FDA, HHS

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 Councils 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 Councils 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-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs monthly Threat Briefing.

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

For Questions or Comments:

Please email us at toc@h-isac.org