Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare **TLP:WHITE** **Alert Id: 696b51d3** **2023-01-19 16:38:38**

This week, Hacking Healthcare begins examining part of the Consolidated Appropriations Act that passed at the end of December. Specifically, we look at the sections that empower the Food and Drug Administration (FDA) to mandate cybersecurity requirements for certain medical devices. After summarizing the new requirements and future engagement, we provide some background context and breakdown some of the more important provisions.

Welcome back to *Hacking Healthcare*.

End of Year Appropriations Act Includes FDA Medical Device Cybersecurity Requirements

Among the wide-ranging provisions from the year-end Appropriations Act that was signed into law at the end of December, is a section that grants the Food and Drug Administration (FDA) new authorities related to medical device cybersecurity. The specific provisions go into effect relatively soon and include the need to provide the FDA with a software bill of materials (SBoM).

Section 3305 of the Consolidated Appropriations Act (Act) amends the Federal Food, Drug, and Cosmetic Act (FFDC) to include a section on Ensuring the Cybersecurity of Medical Devices. The text states that any person "who submits an application or submission under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device under this section shall include such information as the Secretary may require to ensure that such cyber device meets the cybersecurity requirements [listed in the following subsections]."[i]

New Requirements

The text requires that the sponsor of an application or submission related to the sections noted above “shall” do the following:[ii]

- Submit to the Secretary [of HHS] a plan to monitor, identify, and address, as appropriate, in a reasonable time, post market cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures

- Design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available post market updates and patches to the device and related systems to address –
  1. On a reasonably justified regular cycle, known unacceptable vulnerabilities; and
  2. As soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks

- Provide to the Secretary [of HHS] an SBoM, including commercial, open-source, and off-the-shelf software components

- Comply with such other requirements as the Secretary [of HHS] may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure

Cyber Device Definition

The text goes on to define cyber device as one that:

- Includes software validated, installed, or authorized by the sponsor as a device or in a device

- Has the ability to connect to the internet

- Contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

The text also provides the Secretary [of HHS] the authority to exempt devices, or entire categories of devices, from these requirements.

Effective Date

The effective date of these requirements is relatively soon. The Act itself was signed into law on December 29th, and the security noted above are to take effect 90 days from that point, meaning by the end of March. Any submissions sent before that date are not subject to the new requirements.

Future Engagement

The Act also requires that the Secretary of HHS and CISA update either their guidance in the *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* document, or a successor document, within two years and "periodically thereafter as appropriate."[iii] Updating this guidance is to include solicitation of feedback "from device manufacturers, health care providers, third-party-device servicers, patient advocates, and other appropriate stakeholders."[iv]

Additionally, within 180 days of the enactment of the act, roughly the end of June, the Secretary of HHS is to update public information regarding improving medical device cybersecurity. This information is to be updated annually. The information provided must include:

- information on identifying and addressing cyber vulnerabilities for health care providers, health systems, and device manufacturers
- How such entities may access support through the Cybersecurity and Infrastructure Security Agency and other Federal entities, including the Department of Health and Human Services, to improve the cybersecurity of devices.

Finally, the Government Accountability Office (GAO) is required to publish a report that identifies challenges for cybersecurity in devices. This report is to examine:

- Challenges for device manufacturers, health care providers, health systems, and patients in accessing Federal support to address vulnerabilities across Federal agencies
- How Federal agencies can strengthen coordination to better support cybersecurity for devices
- Statutory limitations and opportunities for improving cybersecurity for devices.

Action & Analysis

Included with H-ISAC Membership

Congress

Tuesday, January 17th:

- No relevant hearings

Wednesday, January 18th:

- No relevant hearings

Thursday, January 19th:

- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

[i] https://www.congress.gov/bill/117th-congress/house-bill/2617/text

[ii] https://www.congress.gov/bill/117th-congress/house-bill/2617/text

[iii] https://www.congress.gov/bill/117th-congress/house-bill/2617/text

[iv] https://www.congress.gov/bill/117th-congress/house-bill/2617/text

[v] https://www.fda.gov/media/72154/download

[vi] https://www.politico.com/newsletters/weekly-cybersecurity/2023/01/03/congress-gears-up-for-fight-over-key-surveillance-program-0007604

[vii] https://www.politico.com/newsletters/weekly-cybersecurity/2023/01/03/congress-gears-up-for-fight-over-key-surveillance-program-0007604

[viii] https://www.politico.com/newsletters/weekly-cybersecurity/2023/01/03/congress-gears-up-for-fight-over-key-surveillance-program-0007604

[ix] https://www.politico.com/newsletters/weekly-cybersecurity/2023/01/03/congress-gears-up-for-fight-over-key-surveillance-program-0007604

Reference(s): congress, Politico, FDA

Report Source(s): Health-ISAC

Tags: Hacking Healthcare, Medical Devices, FDA, Congress, cybersecurity

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.