JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE RAPIDLY EVOLVING AND CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog January 2024

GAO REPORT RECOMMENDS GREATER COORDINATION BETWEEN FDA AND CISA REGARDING MEDICAL DEVICE CYBERSECURITY

GAO RECEIVES MANDATE FOR CYBERSECURITY REPORT

The Consolidated Appropriations Act of 2023 was a watershed moment for medical device cybersecurity regulation. The FD&C Act was amended to give the FDA the authority to reject medical device premarket submissions based solely on cybersecurity criteria which was explicitly (and implicitly) identified in the newly amended law. In September of 2023, the FDA released *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*, a finalized guidance which provided medical device manufacturers with recommendations to meet the cybersecurity regulations now present in the amended FD&C Act. These developments were the catalysts for the immediate creation or augmentation of many medical device manufacturer's premarket cybersecurity documentation processes, and the change caught many by surprise as it appeared a sudden shift in regulatory compliance criteria and FDA authority. While the cybersecurity documentation criteria for medical device premarket submission documentation mandated through the Consolidated Appropriations Act of 2023 received a great deal of attention, the Act contained several other long-term provisions which will have a significant impact on the regulatory landscape for medical device cybersecurity. One such provision, section 524B(g), stated the following:

"GAO REPORT. —Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall publish a report identifying challenges in cybersecurity for devices, including legacy devices that may not support certain software security updates. Through such report, the Comptroller General shall examine—

(1) challenges for device manufacturers, health care providers, health systems, and patients in accessing Federal support to address vulnerabilities across Federal agencies;

(2) how Federal agencies can strengthen coordination to better support cybersecurity for devices; and

(3) statutory limitations and opportunities for improving cybersecurity for devices."

ONE YEAR LATER: THE FINDINGS

The GAO report, titled "MEDICAL DEVICE CYBERSECURITY-Agencies Need To Update Agreement to Ensure Effective Coordination" was released on December 21st of 2023. GAO selected 25 non-federal entities representing healthcare providers, patients and medical device manufacturers and interviewed those entities regarding "challenges in accessing federal cybersecurity support". GAO also "assessed agency documentation

John Ward – Cyberblog January 2024
GAO REPORT RECOMMENDS GREATER COORDINATION BETWEEN FDA AND CISA REGARDING MEDICAL DEVICE CYBERSECURITY

and compared coordination efforts and against leading collaboration practices; reviewed relevant legislation and guidance; and interviewed agency officials".

Among the primary findings of the GAO report was that an agreement made between the FDA and the Cybersecurity and Infrastructure Security Agency (CISA) in 2018 which addressed leading practices for cooperation in the space needs to be updated to address "organizational and procedural changes" that have occurred in the five years since. At the time of the original agreement CISA was known as the National Protection and Programs Directorate at the Department of Homeland Security and the FDA had not been granted the statutory authority that it currently holds following the passage of the Consolidated Appropriations Act of 2023. Both FDA and CISA agreed with this finding.

The GAO report additionally found that there are limitations in the FDA's authority over medical device cybersecurity, even after the significant augmentation to their statutory capabilities following the amendment of the FD&C Act. The GAO reported that the FDA's authority regarding cybersecurity in medical devices since October 2023 solely applies to premarket applications made since that time. The GAO report identified limitations in the FDA's authority of cybersecurity in medical devices pertaining to both legacy devices and "healthcare organization usage or maintenance of these devices".

GAO found that the health systems, providers, and patients that were interviewed as part of the report largely reported "challenges in accessing federal support to address cybersecurity vulnerabilities that threaten medical devices". This included challenges understanding vulnerability communications from federal agencies and/or a lack of awareness of federal contacts or resources. GAO reported that the FDA has taken steps to address these challenges, such as partnering with industry leaders for an incident response playbook and making their contact information publicly available. Furthermore, the GAO report found that "FDA has developed resources for vulnerability communications to patients and supported the Healthcare and Public Health Sector Coordinating Council's Cybersecurity Working Group" (HSCC).

IMPACT AND LOOKING AHEAD

The Consolidated Appropriations Act of 2023 appears to have anticipated these findings. In addition to mandating the GAO report discussed in this blog (Sec. 524B(g)) Sec. 524(e) and Sec. 524B (f) provide the

John Ward – Cyberblog January 2024
GAO REPORT RECOMMENDS GREATER COORDINATION BETWEEN FDA AND CISA REGARDING MEDICAL DEVICE CYBERSECURITY

framework for increased collaboration between the FDA and CISA, as well as an emphasis on publicly available information for stakeholders intending to access information and/or support regarding medical device cybersecurity, respectively. Sec. 524(e) specifies that the Secretary of the HHS "in consultation with" the Director of CISA, will update their premarket cybersecurity guidance for medical devices within 2 years and periodically thereafter as needed. These updates will be made following consultation with stakeholders such as device manufacturers, healthcare providers and patient advocates. Sec. 524(f) mandates that the Secretary of HHS will "update public information provided by (the FDA), including on the website of the (FDA) with information regarding improving cybersecurity of devices" at least annually. This includes information on "identifying and addressing cyber vulnerabilities for healthcare providers, health systems, and device manufacturers, and how such entities may access support through (CISA) and other federal entities…to improve the cybersecurity of devices".

This is a critical time in the medical device (and general critical infrastructure) cybersecurity regulatory landscape. Although the GAO report is not designed to make any immediate regulatory changes as the Consolidated Appropriations Act did it is a significant document for understanding the federal government's thinking and ambition in an evolving regulatory landscape. While the amendment to the FD&C Act and finalized cybersecurity guidance of 2023 caught many stakeholders by surprise, those who had been paying attention to the critical infrastructure regulatory environment in the United States over the past several years were able to anticipate many of the changes. Although prior to the Consolidated Appropriations Act of 2023 the FDA had little statutory authority regarding medical device cybersecurity, premarket draft guidances dating back to 2014 provided interested stakeholders with industry best practices regarding cybersecurity in medical devices as well as an understanding of the evolving cybersecurity landscape in the healthcare sector.

The GAO report identified that the FDA has limited statutory authority regarding cybersecurity in legacy devices and healthcare networks, but they have not been idle in these areas. The previously mentioned HSCC provides significant resources to "identify and mitigate systemic risks that affect patient safety, security, and privacy, and consequently national confidence in the healthcare system". They provide an annual report and were responsible for the *Medical Device and Health IT Joint Security Plan*. While the GAO report identified the *MITRE Playbook for Threat Modeling Medical Devices*, FDA has also worked with MITRE to develop the *Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook* as well as *Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks*.

END OF JANUARY 2024 BLOG

