SCIENCES AND CONSULTING

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 July 2023

RECENT BIDEN ADMINISTRATION CYBERSECURITY INITIATIVES AND WHAT TO EXPECT WITH YOUR NEXT FDA SW SUBMISSION

NEW 2023 FEDERAL CYBERSECURITY STRATEGY AND IMPLEMENTATION PLAN

2023 has been a significant year in critical infrastructure cybersecurity. The Biden administration issued the *National Cybersecurity Strategy* in March and the *United States' National Cybersecurity Implementation Plan* in July. Both documents are indicative of a broad awareness of the vulnerable state of both public and private digital systems and the desire to address these vulnerabilities. The SolarWinds hack of 2020, in addition to the JBS meat system and Colonial Pipeline ransomware attacks of 2021, were highly publicized instances of cybercrime and cyber espionage and the significant consequences of a hack. Both the *National Cybersecurity Strategy* and the *National Cybersecurity Implementation Plan* aim to provide a coordinated security framework for all stakeholders who rely on digital systems for privacy, security, and safety.

The president's strategy and plan come at a critical time for healthcare sector cybersecurity following several significant incidents. In March of 2023 Independent Living Systems (ILS), a healthcare administrations and managed care solutions provider based in Miami, notified users of a breach that occurred between June and July of 2022. HCA Healthcare announced in July that the personal (and potentially health) information of potentially tens of millions of people had been stolen and put up for sale. Perhaps most egregiously of all patients of the Lehigh Valley Health Network (LVHN) had their personal data and "…medical photos…depicting patients' naked breasts in various angles and positions" released onto the internet by hackers when LVHN refused to pay during a ransomware attack in February, indicating what Lily Hay Newman warns is a "heinous" new phase of ransomware attacks. Chainalysis, a blockchain analysis firm, reported in July that cryptocurrency-related ransomware is on the rise and has already reached 90% of the cumulative ransomware revenue generation of the entirety of 2022.

PRIVATE-PUBLIC SECTOR CYBERSECURITY COLLABORATION

Private-Public sector collaboration has long been a key component of a robust and effective cybersecurity policy as many sectors of critical infrastructure are largely made up of privately owned and operated entities. These entities can be legally compelled to implement and adhere to cybersecurity activities but that requires regulation through legislation, which can be unpopular with industry, slow, and of an uncertain outcome. Despite the resources provided by CISA, Information Sharing Organizations (ISAOs) and Information Sharing and Analysis Centers (ISACs), many in the private sector do not engage with these federal or federally sanctioned entities for sector-specific cyber threat information. The *National Cybersecurity Strategy*, released to the public on March 1st of 2023, identified five pillars meant to "build and enhance collaboration" in the national cybersecurity posture:

John Ward – Cyberblog April 2023

RECENT CONGRESSIONAL LEGISLATION EXPANDS FDA AUTHORITY FOR CYBERSECURITY PREMARKET SUBMISSION REQUIREMENTS

- Defend Critical Infrastructure
- Disrupt and Dismantle Threat Actors
- Shape Market Forces to Drive Security and Resilience
- Invest in a Resilient Future
- Forge International Partnerships to Pursue Shared Goals

The *National Cybersecurity Strategy Implementation Plan (NCSIP)*, released on July 10th 2023 maps over 65 initiatives to these five pillars encompassing eighteen agencies. To ensure the effectiveness of the *Strategy*, the *NCSIP* indicates that the Office of the National Cyber Director (ONCD) will coordinate all the activities of the *NCSIP* and prepare an annual report to the President and Congress on the status of implementation.

2023 FEDERAL CYBERSECURITY STRATEGY IMPACTS FDA REGULATION OF MDMs

The *Strategy* intends to use regulation for the purposes of "expanding the use of minimum cybersecurity requirements in critical sectors to ensure national security and public safety and harmonizing regulations to reduce the burden of compliance" as well as to "enable public-private collaboration at the speed and scale necessary to defend critical infrastructure and essential services". While the *Strategy* and *NCSIP* do not have any immediate regulatory power over private industry, the healthcare sector has been at the forefront of the Biden administration's push to enhance the cybersecurity of critical infrastructure and has already amended (in effect March, 2023) the Federal Food and Drug Cosmetic Act to proactively regulate the healthcare industry in alignment with the cybersecurity objectives present in the *Strategy* and *NCSIP.*

Strategic Objective 3.3-Shift Liability for Insecure Software Products and Services is an important section of the Strategy for medical device manufacturers (MDMs) who by now are well aware of the amendment to the Federal Food and Drug Cosmetic Act for cybersecurity documentation to be included in premarket submissions to the FDA. The strategic objective identifies the need to shift responsibility for cybersecurity away from customers and patients and place the responsibility on the medical device manufacturers. Beginning October 1st, 2023, MDMs will be receiving "Refuse to Accept" responses from the FDA for their premarket submissions if they do not include specific cybersecurity documentation including Software Bills of Material (SBOMs) and postmarket surveillance plans including Coordinated Vulnerability Disclosure (CVD) among other documentation to prove that their medical device is "reasonably cybersecure".

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 April 2023

RECENT CONGRESSIONAL LEGISLATION EXPANDS FDA AUTHORITY FOR CYBERSECURITY PREMARKET SUBMISSION REQUIREMENTS

Any MDM who has submitted a premarket submission since the FD&C Act was amended earlier this year can attest that FDA scrutiny of the cybersecurity contents of their premarket submissions has increased significantly. The amendment to the Food and Drug Cosmetic Act is also indicative of the *Strategy's* cybersecurity objectives by mandating communication and collaboration between federal entities, as well as between federal entities and the public. The Secretary of HHS is now mandated to collaborate with the Director of CISA periodically to evaluate feedback from MDMs, healthcare providers and other appropriate stakeholders including patient advocates to better inform their "*Content of Premarket Submissions for Management of Cybersecurity in Medical Devices"* or a successor document. The GAO has been empowered to publish a report "identifying challenges in cybersecurity for devices" which examines the healthcare cybersecurity challenges for private stakeholders and federal entities regarding challenges in collaborating between each other. The amended FD&C law now mandates the Secretary of HHS to provide and update public information on the FDA website to identify and address cybersecurity vulnerabilities in the healthcare sector and how to access and leverage federal support to improve the cybersecurity of their devices.

HOW WILL ALL THIS IMPACT YOUR NEXT FDA SW SUBMISSION

MDMs would be wise to familiarize themselves with both the *Strategy* and the *NCSIP*. Many in the FDA have been proponents of stronger cybersecurity regulations for premarket submissions and the FDA were early adopters and contributors to the now seemingly-ubiquitous SBOM established in the Biden Administration's Executive Order on Improving the Nation's Cybersecurity. 2022's Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions was largely in alignment with the Biden administration's cybersecurity objectives of the time; it was released as a draft guidance and did not immediately supplant 2014's Final Guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, but has become the basis for the amendments to the Food and Drug Cosmetic Act that could lead to a medical device premarket submission receiving a "Refuse to Accept" and includes the criteria that an MDM must include to indicate that their medical device is "cybersecure". A proactive understanding of the federal cybersecurity posture, goals and objectives can allow for MDMs to anticipate regulatory changes; some MDMs are currently caught playing catch-up with the FD&C Act amendments while those who studied the Executive Order and subsequent 2022 FDA draft guidance were able to more easily adapt to the stricter cybersecurity requirements for their submissions which are now law.

END OF JULY 2023 BLOG