# 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 September 2022
# SIGNIFICANT MEDICAL DEVICE LEGISLATION INTRODUCED TO CONGRESS

**THE BIDEN'S ADMINISTRATION'S FOCUS ON IMPROVING THE CYBERSECURITY OF CRITICAL INFRASTRUCTURE**

On May 21st, 2021 President Biden issued Executive Order (EO) 14028: Improving the Nation's Cybersecurity. The Order signaled the administration's emphasis on effective cybersecurity policy and governance in the Federal sector as it pertains to critical infrastructure in the United States and called for greater oversight, cooperation, and standardization towards that end. Highly visible and consequential cyberattacks on the meat-packing giant JBS' networks and the Colonial Pipeline, both occurring in the same month in which the Order was issued, served to accentuate the need for critical infrastructure cybersecurity oversight and regulation. This need is especially evident in the healthcare sector; according to the FBI Internet Crime Report 2021 saw the healthcare sector experience the most ransomware attacks of any critical infrastructure sector.

In March of 2022 the *Cyber Incident Reporting For Critical Infrastructure Act (CIRCIA)* was signed into law. CIRCIA requires CISA to "develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA". CIRCIA is not yet in effect pending feedback, suggestions and comments from relevant stakeholders. CIRCIA represents a major development in mandated private/governmental interaction during cyber incidents and will ideally allow for CISA to better collect information about the cyber threat landscape and effectively deploy their resources toward affected public and private entities.

In mid-2022 two pieces of bipartisan legislation were introduced to Congress that could prove transformative for medical device cybersecurity if they are ultimately passed. In March of 2022 the *Protecting Medical Devices From Cyber Attacks (PATCH) Act* was introduced to the Senate by Senators Bill Cassidy (R-LA) and Tammy Baldwin (D-WI) with a companion Act introduced in the House of Representatives by Michael C. Burgess (R-TX) and Angie Craig (D-MN). In May of 2022 Senators Jacky Rosen (D-NV) and Todd Young (R-IN) introduced the *Strengthening Cybersecurity for Medical Devices Act*. Approximately one year from the issuance of EO 14028 two significant pieces of legislation are under consideration for the regulation of cybersecurity in the healthcare sector.

**THE PATCH ACT**

According to a press release by Senators Cassidy and Baldwin the PATCH Act is a direct response to the proliferation of ransomware attacks that the healthcare sector has been facing, the consequences of which became even more significant during the COVID-19 pandemic. The PATCH Act seeks to "implement critical cybersecurity requirements for manufacturers applying for premarket approval through the FDA" making

several amendments to Subchapter A of Chapter V of the Federal Food, Drug and Cosmetic Act (21. U.S.C. 351 et seq.) The bill would require medical device manufacturers submitting premarket applications to FDA for "cyber devices" to consider and include processes and procedures relating to the updating and patching of the proposed device throughout its entire lifecycle.

The PATCH Act would also require medical device manufacturers submitting premarket applications to the FDA to include a Software Bill of Materials (SBOM) that would be provided to users and customers. An SBOM is a "nested inventory" which identifies the software components included in a specific medical device design. SBOMs are a cornerstone of EO 14028. The PATCH Act also requires that a Coordinated Vulnerability Disclosure process be established and disseminated to the FDA upon submission of a premarket application, and empowers the Secretary of Health and Human Services by requiring that these submissions for device approval include "…such information as the Secretary determines to be appropriate" and giving the Secretary the power to grant exemptions to this requirement.

**STRENGTHENING CYBERSECURITY FOR MEDICAL DEVICES ACT**

According to a press release by Senators Young and Rosen the purpose of the *Strengthening Cybersecurity for Medical Devices Act* is to "require the U.S. Food and Drug Administration (FDA) to review and update medical device cybersecurity guidelines and suggestions to ensure devices are protected from possible hacking and cyber attacks". The bill, which is made up of four sections, emphasizes a central role for CISA in the reviewing and updating of FDA medical device guidance documents. The bill also establishes communication protocols and intervals between CISA, the FDA and the Secretary of HHS to optimize governance over guidance documents produced and overseen by the FDA regarding medical device cybersecurity, as well as the establishment and maintenance of informational resources to be accessed by stakeholders.

The Act specifies that the Secretary of HHS and the Director of CISA would review and as appropriate (after soliciting and receiving feedback) update the FDA guidance document *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* or a document that would replace it at least every two years. The Secretary of HHS would also be granted the power to update the guidance (after appropriate notice and comments/feedback) without reissuing the guidance. Informational resources are a primary focus of the Strengthening Cybersecurity for Medical Devices Act. The Act specifies that the Secretary of HHS "update(s) public information provided by the FDA website with information regarding improving cybersecurity of medical devices" at least annually and that the Secretary includes information on how to access support

through CISA and other Federal entities. The Act would also require a Government Accountability Office report that would investigate both "challenges for medical device manufacturers, health systems, and patients in accessing Federal support to address vulnerabilities across Federal agencies" and to suggest how "Federal agencies can strengthen coordination to better support cybersecurity for medical devices".

**THE CURRENT STATE AND (POSSIBLE) FUTURE STATE OF MEDICAL DEVICE CYBERSECURITY IN THE U.S.**

The *PATCH Act* and *Strengthening Cybersecurity for Medical Devices Act*, in conjunction with *CIRCIA*, represent a focus on governance, risk management, threat mitigation and vulnerability assessment in the realm of healthcare critical infrastructure cybersecurity through regulatory legislation. *CIRCIA* and the *Strengthening Cybersecurity Medical Device Cybersecurity Act* both indicate an emphasis on CISA's central role in oversight of Federal regulatory bodies regarding cybersecurity as well as an emphasis on private/governmental communication and resource sharing which is invaluable in an environment where a significant portion of critical infrastructure is owned and operated by private entities. The *PATCH* act seeks to codify as law steps that the FDA has already taken in their most recent draft guidance on the *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* which was issued in 2022; in particular this guidance already includes requirements on SBOMs.

While it is far from a given that either the *PATCH Act* or *Strengthening Cybersecurity Medical Device Cybersecurity Act* will be passed, it is clear that Congress is attempting to apply the core principles of EO 14028 to the larger critical infrastructure cybersecurity landscape and to increase/compel participation and adherence from the private sector. The legislation explored in this blog post confirms that CISA is expected to play a central role in national critical infrastructure cybersecurity. The key elements of this legislation include mandated private entity reporting for cyber incidents, direct CISA oversight of guidance documents and informational resources, and the modification of the US Food, Drug and Cosmetic Act to meet the modern cyber threat landscape.

# John Ward – Cyberblog September 2022
## SIGNIFICANT MEDICAL DEVICE LEGISLATION INTRODUCED TO CONGRESS

**References**


- https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity
- https://www.bbc.com/news/business-57423008
- https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html
- https://www.fbi.gov/news/press-releases/press-releases/fbi-releases-the-internet-crime-complaint-center-2021-internet-crime-report
- https://www.cisa.gov/circia
- https://www.congress.gov/bill/117th-congress/senate-bill/3983/text
- https://www.congress.gov/bill/117th-congress/senate-bill/4336/text
- https://www.cassidy.senate.gov/newsroom/press-releases/cassidy-baldwin-introduce-bill-to-secure-health-care-infrastructure
- https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
- https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions