A black background with a black square

Description automatically generated with medium confidence

Cybersecurity poses a significant threat to our nation’s critical infrastructure, and no sector is impacted more than healthcare. Cyberattacks led by nation-states and other cybercriminals are a regular and growing occurrence. Current headlines depict the detrimental impacts of cyberattacks on patient safety and care and healthcare organizations’ finances. Healthcare is the:

* most attacked,
* highest cost per attack, and
* slowest to identify, detect and respond to cyber incidents.

But it is also **underfunded** and **inadequately prepared**. While other industries only need to protect their computer network, healthcare organizations are significantly more exposed because they deploy millions of medical devices produced by thousands of international manufacturers. Many medical devices are plagued with known exploitable cybersecurity vulnerabilities that go unaddressed. This is partly because manufacturers focus on new product development and unwillingness to address the challenge of legacy devices whose lifespans far exceed those of consumer electronics.

The Alliance for Quality Medical Device Servicing is encouraged by the heightened attention recently directed at healthcare cybersecurity. While multiple cybersecurity bills have been introduced, only one has referred to medical devices, namely the omnibus bill (*H.R.2617 - Consolidated Appropriations Act, 2023*). While this bill is encouraging, the pace of legislative action is far slower than the fast-growing cyber threat capabilities. Very simply, the scope of current legislation does not go far enough to address the risks that continue to mount at an accelerating rate.

Based on these facts, the Alliance seeks immediate action to improve the state of medical device cybersecurity by requiring device manufacturers to:

* **Disclose:** Publicly report new vulnerabilities to a centralized organization accessible by all device users and servicers.
* **Resolve:** Provide validated patches or mitigations for known critical vulnerabilities.
* **Grant Access:** Grant device owners and their service representatives’ access to service information, materials, MDS2s, SBOMs, training, and diagnostic/calibration software to enable detection and reduction of cybersecurity risks, and safe and effective maintenance.

We urge Congress and relevant agencies to take prompt and decisive actions to address cybersecurity for medical devices to protect our healthcare infrastructure and the health of Americans.