June 17, 2021

National Telecommunications and Information Administration
1401 Constitution Avenue, N.W.
Washington, D.C.20230

Via www.regulations.gov

RE: Software Bill of Materials Elements and Considerations *[Docket FDA- 210527–0117]*

Dear Sir or Madam:

MedSec appreciates the opportunity to provide input on the National Telecommunications and Information Administration's Software Bill of Materials Elements and Considerations ("SBOM Elements").

MedSec is the only company of its type focused solely on cybersecurity for hospitals and the medical device manufacturers whose hardware and software play such a crucial role in patient safety. We provide healthcare delivery organizations and medical device manufacturers with a holistic knowledge of cybersecurity – from design and development expertise to regulatory guidance, to implementation on the front lines of patient care. Through MedScan, our software-enabled, medical device cybersecurity system, we help hospitals identify, track, monitor, and protect their connected medical devices, offering real-time alerts to ensure network integrity. MedSec believes that Software Bills of Material (SBOMs) are an important contributor to the way that hospitals can help to manage the cybersecurity of the connected medical devices on their networks and therefore we enable the collection of these documents as part of MedScan's functionality.

Industry cybersecurity experts have identified the importance of understanding the software supply chain and using SBOMs to analyze known cybersecurity vulnerabilities are crucial to managing the growing risk from sophisticated and malicious hackers. SBOM is have been compared to an ingredient label for the software components that are in the medical device. An important part of ensuring visibility to the hidden risks associated with these third-party software vulnerabilities, therefore, is first knowing which products contain the affected software and this is where SBOMs play a critical role.

Some medical device industry's customers are already requiring SBOMs and manufacturers are producing the documents so that hospitals and healthcare providers can make them a part of their cybersecurity strategies. However, the availability and formats of these SBOMs are not consistent. Nor is there a single, efficient way of creating and disseminating SBOMs to the users who need them.

Given the complexities of managing and using SBOM data, more work will be needed to aid the industry in making this process more efficient. We recommend that NTIA continue to collaborate with multi-stakeholders in the NTIA Software Component Transparency effort to provide additional guidance to the affected industries and drive consistency for patients and other healthcare stakeholders. Such collaboration will allow for quicker and more frequent updates to existing tools and the development of new tools based on the evolution of the technology and cybersecurity environments while incorporating feedback from previous efforts and communications.

MedSec would like to thank the NTIA and the Department of Commerce for its consideration of these comments and looks forward to working with the NTIA on this critical area.

Respectfully submitted,

Michelle Jump
Vice President of Security Services, MedSec LLC