AdvaMed
Advanced Medical Technology Association

701 Pennsylvania Avenue, NW
Suite 800
Washington, D.C. 20004–2654
Tel: 202 783 8700
Fax: 202 783 8750
www.AdvaMed.org

April 25, 2022

National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Docket No. 220210-0045: Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

To Whom It May Concern:

The Advanced Medical Technology Association ("AdvaMed") appreciates the opportunity to provide comments in response to the National Institute of Standards and Technology's ("NIST") Request for Information: Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management ("RFI"). AdvaMed represents manufacturers of medical devices, diagnostic products, and health information systems that are transforming health care through earlier disease detection, less invasive procedures, and more effective treatment. Our members range from the smallest to the largest medical technology innovators and companies.

AdvaMed appreciates NIST's desire to improve the Framework. Although the Framework is not directly applicable to the management of risks for medical devices, our members have found portions of the Framework suitable to their management of cybersecurity risks.

Attached is a chart containing our responses to relevant RFI questions.

AdvaMed would like to thank NIST for its consideration of these comments. Please do not hesitate to contact me at [redacted] if you have any questions.

Respectfully submitted,

/s/

Zachary A. Rothstein, J.D.
Senior Vice President
Technology and Regulatory Affairs

Attachment

AdvaMed Comments

Evaluating and Improving NIST Cybersecurity Resources:
The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Line Number	Comment/Proposed Change
Question 1: The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.	The Framework is very useful, particularly for companies with limited cybersecurity experience; however, we believe there would be a benefit for a firm to attest compliance to the Framework, similar to a standard.
Question 2: Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?	• It would be helpful for the Framework to discuss the effort required to progress from one security rating to another. • It would also be helpful if Federal agencies advanced common usage to the Framework.
Question 3: Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).	The Framework is not universally applicable and requires customization for certain environments (*e.g.*, manufacturing, cloud, IoT, and product security).
Question 4: Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.	• Guidance on the Framework's use in various environments (*e.g.*, internal enterprise versus customer facing). • Cross-walks and/or comparisons to similar international standards such as ISO 27001/27002.
Question 6: Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful.	Creating end-point, manufactured device or product oriented mapping to show how a manufactured product can be designed and built within the Framework.
Question 9: There are numerous examples of international adaptations of the Cybersecurity Framework by other countries. The continued use of	Align, map and/or reference NIST special publications that support elements of the Framework. And to further harmonize with international

Line Number	Comment/Proposed Change
international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience can promote innovation and competitiveness while enabling organizations to more easily and effectively integrate new technologies and services. Given this importance, what steps should NIST consider to ensure any update increases international use of the Cybersecurity Framework?	standards, additional information should be included for privacy-related measures.
Question 11: National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?	Standardization on certification of origin and integrity of parts.
Question 13: Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional approaches, tools, standards,guidelines, or other resources that NIST should consider to achieve greater assurance throughout the software supply chain, including for open-source software?	There are gaps in assessing whether supply and component parts are free from bugs and malware.