From: **Rothstein, Zach**
Date: Fri, Apr 7, 2017 at 11:16 AM
Subject: Comments: Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Dear Sir or Madam:

Please find attached comments on behalf of the Advanced Medical Technology Association (AdvaMed) in response to the above mentioned docket.

Please do not hesitate to contact me should you have any questions.

Regards,

Zach Rothstein, Esq.
Associate Vice President
Technology & Regulatory Affairs
AdvaMed
701 Pennsylvania Ave, NW, Suite 800
Washington, DC 20004

[Attachment Copied Below]

April 7, 2017

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

Re: Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity

Dear Sir or Madam:

The Advanced Medical Technology Association ("AdvaMed") appreciates the opportunity to provide comments in response to the National Institute of Standards and Technology's ("NIST") Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity ("Framework"). 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 and its member companies are committed to the proactive management of cybersecurity risks as part of the development and postmarket management of medical technologies. Medical device manufacturers address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment, maintenance and disposal of the device and associated data. Similarly, manufacturers implement proactive measures to manage medical device cybersecurity, including but not limited to routine device cyber maintenance, assessing postmarket information, employing risk-based approaches to characterizing vulnerabilities, and timely implementation of necessary actions.

AdvaMed appreciates NIST's efforts to improve cybersecurity risk management and the opportunity to provide NIST with comments on the Framework.[1] Although the Framework is not directly applicable to the management of risks for medical devices, our members have found portions of the Framework helpful. Moreover, the U.S. Food and Drug Administration ("FDA"), whom we commend for its proactive leadership role over medical device cybersecurity, has utilized the Framework in its work to ensure that medical device cybersecurity is considered and addressed throughout all stages of product design and use. For example, in 2014, FDA released final guidance concerning premarket cybersecurity-related issues device manufacturers must consider when designing a connected medical device.[2] In addition, in December 2016, FDA released final guidance concerning the postmarket management of medical device cybersecurity.[3]

We provide below a response to the questions posed in the Framework on page iii. Additional detailed comments are provided in the attached document.

[1] *See, e.g.,* AdvaMed Comments to NIST: Views on the Framework for Improving Critical Infrastructure Cybersecurity: Notice; Request for Information (Feb. 9, 2016).

[2] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff (Oct. 2, 2014).

[3] Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff (Dec. 28, 2016).

1. Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?

Based on identified "Areas for Development, Alignment, and Collaboration" in the *NIST Roadmap for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), and recognizing the importance of issuing timely guidance to critical infrastructure sectors, we do not believe additional items should be addressed by Version 1.1. We are particularly pleased to see a discussion of Cyber Supply Chain Risk Management ("SCRM"). SCRM is a valuable addition to the Framework because medical device manufacturers may rely on components, subassemblies, software, firmware, and services sourced from third-party suppliers.

2. How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?

As stated above, the additional discussion of SCRM is the most impactful change for AdvaMed members. Changes to the Identity Management and Access Control (PR.AC) category align with industry norms and highlight this aspect of the Protect (PR) function for critical infrastructure stakeholders.

3. For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?

We believe that the addition of SCRM and the changes made to the Identity Management and Access Control category will increase use of the Framework.

However, we are concerned that the update characterized on page ii as a "Better explanation of the relationship between Implementation Tiers and Profiles" will discourage use of the Framework. Related modifications to the Framework do not aid in explaining this relationship. For example, the third paragraph of section 2.2 includes a new sentence: "However, Tier selection and designation naturally affect Framework Profiles." The inclusion of this statement should be reconsidered. If a Profile "can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario," then a Tier should be based on this customization. As we stated in our previous comments to NIST on Feb. 9, 2016 (Question #13), "While the Framework Core is easily understood, stakeholders would benefit from informative examples for the Framework Implementation Tiers and Framework Profile."

4. For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?

This question generally does not apply to AdvaMed and its member companies. Most of our members use the Framework in some manner because it is referenced in FDA's guidance titled, *Postmarket Management of Cybersecurity in Medical Devices*.

5. Does this proposed update adequately reflect advances made in the Roadmap areas?

Yes, however, we believe the Roadmap should be revised (see response to question 7).

6. Is there a better label than "version 1.1" for this update?

We support use of the term, Version 1.1.

7. Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?

The Roadmap should be revised to address the emergence of Internet of Things ("IoT") architectures and the related potential for global distributed denial of service attacks. Both of these topics were briefly discussed in a November 14, 2016 memorandum addressed to members of two subcommittees of the U.S. House of Representatives.[4] IoT has also been addressed in other U.S. Government publications.[5]

Section 3 of the Roadmap, "Strengthening Private Sector Involvement in Future Governance of the Framework," should be removed unless NIST intends to relinquish its leadership role over the Framework. We believe discussion of "an ideal transition partner" is out of place in a Roadmap whose primary purpose is to identify cybersecurity trends. As stated in our previous comments to NIST filed by AdvaMed on Feb. 9, 2016: "AdvaMed believes NIST is the appropriate organization to develop a high-level Framework applicable to all critical infrastructure sectors."

[4] http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-20161116-SD005-U2.pdf.

[5] See, e.g., https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf; http://latta.house.gov/uploadedfiles/iot_working_group_white_paper.pdf.

*		*		*

AdvaMed would like to thank NIST for its consideration of these comments. Please do not hesitate to contact me at 202-434-7224 or zrothstein@advamed.org if you have any questions.

Respectfully submitted,

/s/

Zachary A. Rothstein, Esq.
Associate Vice President
Technology and Regulatory Affairs

Attachment

#1	Page 2, Executive Summary, second to last paragraph	Change: “NIST will continue coordinating industry as directed in the Cybersecurity Enhancement Act” to (additions underlined): “NIST will continue ~~coordinating industry~~ to coordinate closely and regularly with relevant private sector personnel and entities, critical infrastructure owners and operators, and other relevant industry organizations as directed in the Cybersecurity Enhancement Act”	Rationale: Provides a more comprehensive view of NIST’s coordination responsibilities as required by the Act (15 U.S.C. § 272(e)(1)(A)(i)).
#2	Page 9, section 2.2, second paragraph	Change: “cyber supply chain risk management needs, and organizational….” to (additions underlined): “cyber supply chain risk management ~~needs~~ capabilities, and organizational….”	Rationale: The “needs” of an organization are only one factor. Tier selection should be based on overall organizational capabilities in this area.
#3	Page 9, section 2.2, third paragraph	Change: “However, Tier selection and designation naturally affect Framework Profiles. The risk disposition expressed in a desired Tier should influence prioritization within a Target Profile. Similarly, the organizational state represented in an assessed Tier will indicate the likely findings of an assessed Profile, as well as inform realistic progress in addressing Profile gaps.” to: “~~However, Tier selection and designation naturally affect Framework Profiles. The risk disposition expressed in a desired Tier should influence prioritization within a Target Profile. Similarly,~~ ~~t~~The organizational state represented in an assessed Tier will indicate the likely findings of an assessed Profile, as well as inform realistic progress in addressing Profile gaps.”	Rationale: The proposed deletion clarifies the primary message of the paragraph and reduces the potential for confusion.

#4	Page 14, section 3.0, third paragraph	Change: "The Framework can be applied in design, build/buy, deploy, operate, and decommission system lifecycle phases . . . ." to (additions underlined): "Sector-Specific Agencies can adapt ~~T~~the Framework can be applied to guide its application in design, build/buy, deploy, operate, and decommission system lifecycle phases . . . ."	Rationale: Section 8(b) of Executive Order 13636 recognizes the existence of "sector specific risks and operating environments" and the role of Sector-Specific Agencies to develop implementation guidance or supplemental materials. Accordingly, the Framework should not incorporate broad statements about its applicability without acknowledging the role of Sector-Specific Agencies. See also AdvaMed's previous comments to NIST: "The Framework does not account for sector-specific limitations and requirements. The Federal agency responsible for regulating a specific critical infrastructure sector should adapt the Framework to accommodate sector-specific requirements and limitations."
#5	Page 21, section 4.0, second paragraph	Change: "Measures are most closely aligned with technical controls, such as the Informative References." to (additions underlined): "Measures are most closely aligned with technical controls, such as those contained within the Informative References."	Rationale: Informative References, such as controls catalogs, offer detailed technical measures that work modularly to complement Framework. This edit would align the sentence with a statement made in the last paragraph of section 4.2.