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

January 19, 2018

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

Re: Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Draft 2

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"), Version 1.1, Draft 2. 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.

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. 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 2013, FDA released final guidance concerning premarket cybersecurity-related issues device manufacturers must consider when designing a connected medical device.[1] In addition, in December 2016, FDA released final guidance concerning the postmarket management of medical device cybersecurity.[2]

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

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

We believe Draft 2 of Version 1.1 of the Framework provides a number of beneficial additions to the document to assist with a firm's cybersecurity risk management. In particular, we are pleased that NIST has included the following content:

1. Supply chain considerations (*i.e.*, cyber SCRM);

2. Additional information and considerations for the Internet of Things ("IoT"), although we believe even more detail could be included for IoT considerations (*e.g.*, NISTIR 8201, *available at* https://csrc.nist.gov/publications/detail/nistir/8201/final);

3. Additional attention and consideration of the concept of "availability" (*e.g.*, PR.PT-5); and

4. Distinguishing between security events and security incidents.

In the attached chart, we provide more detailed comments on Draft 2 for your consideration.

* * *

AdvaMed thanks NIST for its ongoing work related to cybersecurity and refinement of the Framework. 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

AdvaMed Comment Form

Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Draft 2

#	Page/ Section/ Paragraph/ Line[1]	Comment/Proposed Change	Rationale
1	Executive Summary, line 88	Change "… outcomes, and informative references that are common across sectors and critical infrastructure." to:[2] "… outcomes, and informative references that are common across ~~sectors and~~ critical infrastructure sectors."	The phrase "common across sectors" is not accurate and lacks context (i.e., no reference entity is identified for sectorization). The proposed change returns the sentence to that included in the existing Framework (Version 1.0).
2	Executive Summary, lines 95-96	Change "While this document was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community." to: "While this document was developed to improve cybersecurity risk management in critical infrastructure sectors, the Framework can be used by organizations in any ~~sector or~~ community."	Clarifies the intent of the Framework and reduces the potential for confusion introduced by generalizing the term "sectors" in the absence of any context.
3	Line 154	Change "is increasingly used …" to: "are increasingly used …"	Editorial (subject-verb agreement).
4	Lines 171-173	Change "The Framework remains effective and support technical innovation, because it is technology neutral, while also referencing a variety of existing standards, guidelines, and practices that evolve with technology." to:	Editorial (changed structure for clarity).

[1] Line numbers reflect the version of the document "without markup," *available at* https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf.

[2] When applicable, additions are marked as underlined text and deletions are struck. These additions and deletions are also in red font.

#	Page/ Section/ Paragraph/ Line[1]	Comment/Proposed Change	Rationale
		"Although ~~T~~the Framework is technology neutral, it remains effective and supports ~~technical~~ innovation~~, because it is technology neutral, while also~~ by referencing a variety of existing standards, guidelines, and practices that evolve with technology.	
5	Lines 194-197	Change "While the Framework has been developed to improve cybersecurity risk management as it relates to critical infrastructure, it can be used by organizations in any sector of the economy or society. It is intended to be useful to companies, government agencies, and not-for-profit organizations regardless of their focus or size." to: "While the Framework has been developed to improve cybersecurity risk management ~~as it relates to~~ for critical infrastructure sectors, it can be used by other organizations ~~in any sector of the economy or society. It is intended to be useful to companies, government agencies, and not-for-profit organizations~~ regardless of their focus or size."	Clarifies the intent of the Framework and reduces the potential for confusion introduced by generalizing the term "sectors" in the absence of any context.
6	Lines 335-339	We recommend adding the additional text to recommend that security events are logged when detected: **Detect** – Develop and implement the appropriate activities to identify and record the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events, as well as recording the details of such events, for further investigation. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.	The practice of logging cybersecurity events as they are detected should be called out in the framework core functions under the "Detect" section. The addition of this in the foundational section will help emphasize the importance of logging and recording events for follow-up as well as for capturing important evidence for further investigation.
7	Lines 581-582	Change "The Profile should appropriately reflect criteria within the target Implementation Tier." to: "The Target Profile should appropriately reflect criteria within the target Implementation Tier."	Reduces ambiguity since several types of profiles are described in the document.

#	Page/ Section/ Paragraph/ Line[1]	Comment/Proposed Change	Rationale
8	Line 602	We recommend retitling Section 3.3 to, "Communicating Cybersecurity Requirements with Supply Chain Stakeholders," or creating a new supply chain section altogether.	Due to the significance of supply chain management as well as the amount of content added to this section, it should be called out in its own section or this section should be retitled. The existing section title pointing to "Stakeholders" alone is much too general with the proposed changes.
9	Lines 668-669	Delete the sentence "This transaction varies from cyber SCRM (Section 3.3) in that it may not be possible to impose a set of cybersecurity requirements on the supplier." and change "~~Instead, t~~The objective …" in the sentence that follows.	The sentence "This transaction varies from cyber SCRM (Section 3.3) in that it may not be possible to impose a set of cybersecurity requirements on the supplier." does not align with line 634 "Enacting cybersecurity requirements through formal agreement (e.g., contracts)" which clearly envisions applying cyber SCRM to the purchasing process.
10	Lines 765-766	Change "Making choices about how different portions of the cybersecurity operation should operate setting Target Implementation Tiers," to: "Making choices about how different portions of the cybersecurity operation should ~~operate setting~~ influence the selection of Target Implementation Tiers,"	The existing sentence requires clarification (i.e., the phrase "operation should operate setting").
11	Document page 27, ID.RA-2	Change "Cyber threat intelligence is received from information sharing forums" to: "~~Cyber t~~Threat ~~intelligence~~ and vulnerability information is received from information sharing forums and sources"	The inclusion of vulnerability information is supported by NIST SP 800-53 Rev 4, PM-15 "c. To share current security-related information including threats, vulnerabilities, and incidents." and SI-5 (advisories can include vulnerability information). Information is available from sources other than forums. The proposed change returns the subcategory title to that included in the existing Framework (Version 1.0).
12	Document page 34, PR.DS-8	The Subcategory description is unclear. We recommend changing it to "PR.DS-8: Hardware integrity is verified prior to and during operation," or similar.	We believe this proposed change will clarify the text.