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

February 9, 2016

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

***Re: Docket No. 151103999-5999-01: Views on the Framework for Improving Critical Infrastructure Cybersecurity: Notice; Request for Information***

Dear Ms. Honeycutt:

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: Views on the Framework for Improving Critical Infrastructure Cybersecurity ("Framework 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 learn more about the variety of ways in which the Framework is being used 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 suitable to their management of cybersecurity risks. For example, our members have found Appendix A, Table 2: Framework Core useful as it provides a convenient mapping of Subcategories to Informative References and can be used to validate use of certain consensus standards and NIST publications. Some members have also found Section 3 (How to Use the Framework) useful.

As our comments in the attached chart explain in greater detail, the Framework does not account for sector-specific limitations and requirements. We believe the Federal agency responsible for regulating a specific critical infrastructure sector should adapt the Framework to accommodate sector-specific requirements and limitations. For medical devices, we believe the security requirements must be balanced against the intended use of the product. For example, in the Health Care and Public Health sector, many medical devices are required to be immediately accessible by a physician during an emergency medical procedure, and miniaturized medical devices are often constrained by limited energy storage (*e.g.*, battery life). Ensuring these factors are accounted for in the development of sector-specific requirements is critical to the safe performance of these devices.

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, J.D.
Associate Vice President
Technology and Regulatory Affairs

Attachment

**AdvaMed Comment Form**

**Date:** **February 9, 2016**

**Document Title: Views on the Framework for Improving Critical Infrastructure Cybersecurity: Notice; Request for Information (Docket Number: 151103999–5999–01)**

**Submitters Name:** **Zachary A. Rothstein** **Company:** **Advanced Medical Technology Association (AdvaMed)**

| Question | Comment |
|---|---|
| **USE OF THE FRAMEWORK** | |
| 1. Describe your organization and its interest in the Framework. | From the viewpoint of medical device manufacturers, the Framework provides high-level guidance to federal agencies that regulate critical infrastructure sectors and to private entities that manage corporate information technology (IT) assets.<br>The Framework is not directly applicable to the management of risks (including cybersecurity risks) for medical devices as described in standards such as ISO 14971:2007. |
| 2. Indicate whether you are responding as a Framework user/nonuser, subject matter expert, or whether you represent multiple organizations that are or are not using the 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. Some of our members use the Framework in their corporate IT management policies; however, we have found it difficult to implement the Framework for specific products, such as medical devices. |
| 3. If your organization uses the Framework, how do you use it? (*e.g.*, internal management and communications, vendor management, C-suite communication). | Many of AdvaMed's members do not directly reference the Framework in their policies, processes, or procedures, but may adhere to applicable "Informative References" listed in Appendix A, Table 2: Framework Core.<br>A small subset of our members reference the Framework in their corporate IT management policies. Such members use the Framework as a guide for evaluating the vulnerabilities in and threats to their IT systems. |
| 4. What has been your organization's experience utilizing specific portions of the Framework (*e.g.*, Core, Profile, Implementation Tiers, Privacy Methodology)? | Some members have used Appendix A, Table 2: Framework Core to validate their use of certain consensus standards and NIST publications. |

| | |
|---|---|
| 5. What portions of the Framework are most useful? | Our members have found Appendix A, Table 2: Framework Core most useful as it provides a convenient mapping of Subcategories to Informative References. Some members have also found Section 3 (How to Use the Framework) useful. |
| 6. What portions of the Framework are least useful? | We have not found the Glossary to be particularly useful since it does not provide a source (reference) for each definition. In addition, Figure 2 is not particularly useful because an entity may implement the Framework differently. |
| 7. Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)? | 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. For example, in the Health Care and Public Health sector, many medical devices are required to be immediately accessible by a physician during an emergency medical procedure, and miniaturized medical devices are often constrained by limited energy storage (e.g., battery life). Accordingly, we believe security requirements must be balanced against the intended use of the medical device. *See, e.g.,* GAO Report 16-152 (Dec. 2015) *Critical Infrastructure Protection, Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework* ("For their part, SSAs [sector-specific agencies] for most sectors are developing tailored guidance for implementing the framework in their sectors, and NIST has promoted the framework through public events and its website.").<br>In addition, we believe the Framework should address internal "bad actors" that may compromise or exploit a business's critical system. |
| 8. To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any. | AdvaMed did not receive any data that quantify reduction of medical device risk due to the Framework. |
| 9. What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014? | The Framework, as written, provides high-level guidance to sector-specific agencies and a useful mapping to Informative References. The level of detail is appropriate for this type of document. |

| **POSSIBLE FRAMEWORK UPDATES** | |
|---|---|
| 10. Should the Framework be updated? Why or why not? | Yes. The list of Informative References contained in Appendix A, Table 2, should be periodically reviewed for accuracy because consensus standards and NIST publications are often revised. Additionally, updates may be required to address new types of threats. |
| 11. What portions of the Framework (if any) should be changed or removed? What elements (if any) should be added to the Framework? Please be as specific as possible. | AdvaMed does not believe additional detail should be added to the Framework. As indicated in our comment to question 7, the Federal agency responsible for regulating a specific critical infrastructure sector should adapt the Framework to accommodate that sector's specific limitations and requirements and communicate related guidance to stakeholders in their sector. |
| 12. Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework? | As discussed in our comment to question 10, the list of Informative References contained in Appendix A, Table 2, should be periodically reviewed for accuracy. |
| 13. Are there approaches undertaken by organizations—including those documented in sector-wide implementation guides—that could help other sectors or organizations if they were incorporated into the Framework? | If a sector-specific approach is included in the Framework as a "good practice" example, then related documentation should be placed in a new informative appendix. While the *Framework Core* is easily understood, stakeholders would benefit from informative examples for the *Framework Implementation Tiers* and *Framework Profile*. The use of Tiers and Profiles (including "Current State" and "Target") should be clarified. |
| 14. Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how? | Developments made in the nine areas identified by NIST should be used to inform updates to the Framework. The cybersecurity environment is constantly changing, and a partnership with NIST should be leveraged to update the "Roadmap" as required. |

| | |
|---|---|
| 15. What is the best way to update the Framework while minimizing disruption for those currently using the Framework? | A public review and comment process, conducted in accordance with the Administrative Procedures Act, is the best way to update the Framework. |
| **SHARING INFORMATION ON USING THE FRAMEWORK** | |
| 16. Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful? | Members of AdvaMed frequently use NIST publications (*e.g.*, Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*) to inform their management of cybersecurity risk. SP 800-30 and similar publications provide more detailed information than the Framework. |
| 17. What, if anything, is inhibiting the sharing of best practices? | Consensus standards development organizations (SDOs) focused on cybersecurity have only recently been established. For example, the Association for the Advancement of Medical Instrumentation (AAMI) recently established AAMI SM/WG05 (Device Security Working Group). This group is developing a Technical Information Report (TIR) that includes best practices contributed from a number of participating entities including medical device manufacturers and academia.<br>One challenge related to the sharing of best practices is that threats are constantly adapting in response to new security controls. Other barriers include private sector concerns about liability and the lack of public sector processes to sanitize information (*e.g.*, removal of classified content). |
| 18. What steps could the U.S. government take to increase sharing of best practices? | Best practices are shared by both public and private entities. Private sector organizations such as the National Health Information Sharing and Analysis Center (NH-ISAC) and AAMI play a critical role in sharing best practices and would benefit from an increased level of Federal participation.<br>NIST's Computer Security Resource Center (CSRC) publishes many valuable guidelines and recommendations. The public would benefit from more frequent revisions of certain CSRC publications so that they accurately reflect current best practices. For instance, the most recent version of SP 800-30 (Revision 1) *Guide for Conducting Risk Assessments* was published in September 2012. |

| | |
|---|---|
| 19. What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (*e.g.*, peer-recognition, trade association, consortia, federal agency)? | In addition to our response to question 18, AdvaMed does not believe that a new Federal agency and/or program is necessary to foster an increased level of information sharing. We do believe, however, that additional collaboration in the private sector, including NH-ISAC, AAMI and other ISAOs, may be beneficial. |
| **PRIVATE SECTOR INVOLVMENT IN THE FUTURE GOVERNANCE OF THE FRAMEWORK** | |
| 20. What should be the private sector's involvement in the future governance of the Framework? | The private sector should contribute to governance of the Framework through membership in Federal Advisory Committees such as the Information Security and Privacy Advisory Board (ISPAB). |
| 21. Should NIST consider transitioning some or even all of the Framework's coordination to another organization? | No, AdvaMed believes NIST is the appropriate organization to develop a high-level Framework applicable to all critical infrastructure sectors. |
| 22. If so, what might be transitioned (*e.g.*, all, Core, Profile, Implementation Tiers, Informative References, methodologies)? | N/A |
| 23. If so, to what kind of organization (*e.g.*, not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining? | N/A |

| | |
|---|---|
| 24. How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework? | N/A |
| 25. What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally? | N/A |