TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Rd., Suite 200
Arlington, VA 22201 USA
www.tiaonline.org
Tel: +1.703.907.7700
Fax: +1.703.907.7727

Submitted via www.regulations.gov

September 12, 2013

Food and Drug Administration Center for Devices and Radiological Health
c/o
Division of Dockets Management (HFA-305)
Food and Drug Administration
5630 Fishers Lane, Room 1061
Rockville, MD 20852

RE: Comments of the Telecommunications Industry Association to the Food and Drug Administration's *Draft Guidance for Industry and Food and Drug Administration Staff; Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (Docket No. FDA–2013–D–0616)

Dear Ms. Brady:

The Telecommunications Industry Association ("TIA") congratulates the Food and Drug Administration ("FDA") on its issuance of draft guidance on the content of premarket submissions for the management of cybersecurity in medical devices,[1] and for seeking stakeholder input. The FDA's guidance documents are crucial efforts towards enhancing health care in the United States.

I. Introduction and Statement of Interest

TIA is and has been a standards development organization since its inception in 1988, and is one of the largest SDOs accredited by ANSI. TIA's standards committees create consensus-based voluntary

[1] Food and Drug Administration, *Draft Guidance for Industry and Food and Drug Administration Staff; Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (Docket No. FDA–2013–D–0616), 78 Fed Reg 35940 (Jun. 14, 2013) ("Draft FDA Guidance").

standards for numerous facets of the ICT industry, for use by both private sector interests and government, which are directly affected by the policies of the U.S. Government in the sweeping area of health information technology. Among other areas, TIA's standards committees develop protocols and interface standards relating to current U.S. Government technology priorities in such areas as fiber optics, public and private interworking, telecommunications cable infrastructure, wireless and mobile communications, multimedia and voice over internet protocol ("VoIP") access. TIA's standards reach into areas such as Smart Grid, emergency communications infrastructure, and – of particular relevance to the Draft FDA Guidance – health care ICT and machine-to-machine ("M2M"). TIA's hundreds of member companies provide, develop, manufacture, and supply ICT, including components of, devices used in the healthcare setting. TIA members occupy critical roles in the mHealth community, producing many of the mobile products, medical devices, and health applications which have become increasingly powerful tools for innovative health care solutions. We appreciate the risk that cybersecurity breaches, both intentional and unintentional, present, and our members take steps to evaluate network security and protect networks from cybersecurity risks. These steps include updates that enhance the monitoring of network activity for unauthorized use, the updating of security patches, and the execution of cybersecurity incident response plans. While device manufacturers are not always required to do this,[2] these steps are primarily taken to gain competitive advantage due to market effects.

I. The FDA Should Clarify the Applicability of the Guidance to Premarket Submissions

TIA believes that it would be unreasonably burdensome from a practical and cost perspective for medical device manufacturers to have to revisit all of their devices and software already released into the stream of commerce. We therefore urge the FDA to clarify in its final guidance that this guidance is intended to apply prospectively to future premarket submissions, and that the

[2] Device manufacturers may offer a service to a customer covered by HIPAA and HITECH (called "covered entities" in HIPAA), that creates a "Business Associate" relationship with the covered entity. In that situation, the device manufacturer would be subject to HIPAA and HITECH.

guidance should not be applied to medical devices already in the marketplace or to medical devices which have received premarket approval prior to the issuance of the Draft FDA Guidance. We also request further clarification on whether a premarket notification 510(k) can reference cybersecurity standards if the predicate device does not currently employ such standards, since the 510(k) is intended to demonstrate substantial equivalence to a predicate device.

Moreover, the Draft FDA Guidance states that a manufacturer should provide "[a]ppropriate documentation to demonstrate that the device will be provided to purchasers and users free of malware."[3] Because a medical device may pass through numerous entities before it is provided to a purchaser or user, FDA should clarify the information that is necessary to support this statement. At a minimum, FDA should not require a device manufacturer to attest to malware after the device is handled by a third-party.

II. The Draft FDA Guidance Should Incorporate the Use of Cybersecurity Standards in the Medical Device Setting

The draft guidance stands at the intersection of two increasingly important regulatory trends that reflect basic technological and economic shifts: the proliferation of cybersecurity standards, and the development of technologies for the movement of nearly every aspect of health and medical practices into the digital domain. TIA urges that the Draft FDA Guidance reflect the priority for U.S.-based technologies' continued success in the global marketplace, which has been enabled through the development of internationally-used standards and best practices. The Draft FDA Guidance should also recognize that the adoption and use of open and voluntary standards is a long-standing federal policy that promotes effective and efficient technology and innovation in the marketplace.[4]

---

[3] Draft FDA Guidance at 5.

[4] *See* OMB Circular A-119 Revised, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities (rev. Feb. 10, 1998) (OMB Circular A-119) *available at* http://www.whitehouse.gov/omb/rewrite/circulars/a119/a119.html.

Consistent with these themes, we urge FDA to recognize that that the global nature of the ICT industry necessarily requires a global approach to address cybersecurity concerns, and can only be secured through an industry-driven adoption of best practices and global standards. The FDA's efforts in this area should also incorporate other Federal agencies' efforts[5] as well as North American SDOs and companies to ensure that any standards, regardless of where they are developed, be viewed as "international" standards if they are globally adopted; these standards may additionally be appropriate for designation as FDA-recognized consensus standards.[6] The final guidance at issue should include language reflecting these priorities.

III. The FDA Should Clarify in its Final Guidance that it Will Not Typically Review Medical Device Software Changes Made Solely to Strengthen Cybersecurity

TIA notes that an issue of concern in the Draft FDA Guidance is its effect on software modifications made to a medical device after it is already in the stream of commerce. This is a serious compliance concern for medical device manufacturers as the update may trigger modification requirements[7] to the FDA, and could result in having to submit a new related premarket submission. Given the resources and time required to prepare a premarket submission, as well as medical device user fees associated with premarket submissions, this could result in a substantial burden to companies.

Given the dynamic world of threats and responses that occur and are addressed in ICT product software, software modifications are needed for devices constantly. Manufacturers understand

---

[5] For example, there are numerous activities across the Federal government pursuant to the February 2013-released cybersecurity-themed Executive Order, such as the development by the National Institute of Standards and Technology of a Cybersecurity Framework. *See* Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, rel. Feb. 12, 2013.

[6] For a current list of FDA-recognized consensus standards, see the Recognized Consensus Standards Database at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm.

[7] *See* 21 C.F.R. 806.

that for such converged devices that are also medical devices, the potential damage to patients makes keeping such products as effective and secure as possible, and many system integrators will rely on their components to perform this task. These updates almost universally have no bearing on the medical application of the device and are strictly security-themed. To overzealously require reporting requirements for these changes would negatively impact those medical device manufacturers and healthcare providers that rely on them.

Previous guidance from the FDA in 2005 that addressed software maintenance actions required to address cybersecurity vulnerabilities for networked medical devices, particularly those that incorporate off-the-shelf ("OTS") software, has stated that device manufacturers will very likely not have to report updating software in medical devices with cybersecurity patches because "most software patches are installed to reduce the risk of developing a problem associated with a cybersecurity vulnerability and not to address a risk to health posed by the device."[8] Specifically addressing the risk of triggering another premarket submission as the result of such an update, the FDA also stated in the same document that "[i]n general, review is necessary when a change or modification could significantly affect the safety or effectiveness of the medical device."[9] The FDA has not annulled this guidance. In the Draft FDA Guidance at hand, and TIA believes that this approach is appropriate. TIA agrees that the FDA should not typically need review medical device software changes made solely to strengthen cybersecurity.

Based on feasibility and the previous precedent the FDA has established, we urge the FDA to clearly state in its final guidance document that it will not typically need review medical device software changes made solely to strengthen cybersecurity.

---

[8] FDA, *Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software* (Jan. 14, 2005) at 5 ("FDA COTS Device Guidance").

[9] *Id.* at 4.

IV. Conclusion

We appreciate the dutiful steps that the FDA has taken to enable enhanced innovation in the development and proliferation of home use devices. We urge you to consider the positions stated above, and to contact the undersigned with any questions.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: */s/ Danielle Coffey*

Danielle Coffey
Vice President, Government Affairs

Mark Uncapher
Director, Regulatory and Government Affairs

Brian Scarpelli
Senior Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 Court House Road
Suite 200
Arlington, VA 22201
(703) 907-7700

September 12, 2013