mdpc medical device privacy consortium

May 24, 2016

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930

Re: SP800-150 – Guide to Cyber Threat Information Sharing

To Whom It May Concern:

The Medical Device Privacy Consortium ("MDPC") writes in support of NIST's recently-released draft of its *Guide to Cyber Threat Information Sharing* ("*Guide*"). The MDPC is composed of medical device manufacturers concerned about issues related to privacy and data security. Cybersecurity is more important than ever for the medical device industry, and NIST's draft provides welcome guidance as MDPC members continue to develop and implement cutting-edge security and privacy practices.

As NIST refines the *Guide* in response to industry comments, the MDPC would like to take the opportunity to call attention to the FDA's recently issued draft guidance entitled *Postmarket Management of Cybersecurity in Medical Devices*.[1] The FDA guidance leverages the agency's considerable experience with the medical device industry to address issues that industry participants face on a regular basis. Further, we note that the FDA encourages the sharing of information about cybersecurity threats and vulnerabilities that may affect the safety, effectiveness, integrity and security of medical devices and the surrounding Health IT infrastructure. It is MDPC's belief that consistency across industry standards is a key component in fostering widespread adoption of best practices and facilitating technological advancement. Accordingly, MDPC respectfully requests that NIST seeks to harmonize its guidance with the standards promulgated by the FDA to the greatest extent possible.

The FDA guidance encourages manufacturer participation in an Information Sharing and Analysis Organization ("ISAO"). Although this type of organization is not mentioned in the *Guide*, similar concepts are addressed and we encourage NIST to work with the FDA in defining the role of an ISAO and its responsibilities.

In addition, due to the nature of the research conducted in the medical device field, much of the relevant cyber threat information available to MDPC members may include patient data. With respect to such data, the draft *Guide* directs readers to the NIST de-identification standards. In the past, NIST's de-identification standards have provided important guidance to MDPC members as they developed procedures for de-identifying information and handling such de-identified data. However, it is not entirely clear how the de-identification standards would apply in the context of cyber threat information sharing. Further, NIST's draft *Guide* does not elaborate on this issue beyond citing to the existing de-

[1] See Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff, FDA (Jan. 22, 2016), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

identification standards. Thus, MDPC hopes that the final version of the *Guide* incorporates additional clarification on the appropriate de-identification procedures for medical device companies and other health industry participants to follow with respect to information that will be shared via a cyber threat information sharing program.

MDPC is otherwise supportive of the *Guide* as written and believes it will be an instructive and valuable tool for industry participants as they seek to efficiently address cyber threats and protect personal data. MDPC thanks NIST for its careful attention to the issues raised in these comments and looks forward to working with NIST as it continues adapting its cybersecurity guidance to an evolving cyber threat landscape.

Sincerely,

The Medical Device Privacy Consortium