DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. FDA-2014-N-1286]

Collaborative Approaches for Medical Device and Healthcare Cybersecurity; Public Workshop; Request for Comments

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice of public workshop; request for comments.

The Food and Drug Administration (FDA) is announcing the following public workshop entitled "Collaborative Approaches for Medical Device and Healthcare Cybersecurity". FDA, in collaboration with other stakeholders within the Department of Health and Human Services (HHS) and the Department of Homeland Security (DHS), seeks broad input from the Healthcare and Public Health (HPH) Sector on medical device and healthcare cybersecurity. The vision for this public workshop is to catalyze collaboration among all HPH stakeholders. Participants will identify barriers to promoting cooperation; discuss innovative strategies to address challenges that may jeopardize critical infrastructure; and enable proactive development of analytical tools, processes, and best practices by the stakeholder community in order to strengthen medical device cybersecurity.

Dates and Times: The public workshop will be held on October 21 and 22, 2014, from 9 a.m. to 5 p.m.

Location: The public workshop will be held at the National Intellectual Property Rights Coordination Center Auditorium, 2451 Crystal Dr., suite 200, Arlington, VA 22202. Entrance for the public workshop participants is through the main doors which face Crystal Drive. Upon arrival at the facility, participants should visit the registration table to check in. For parking,

participants may choose from a number of pay garages, including one directly beneath the facility.

Contact Person: Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5418, Silver Spring, MD 20993, 301-796-6937, FAX: 301-847-8510, email: Suzanne.Schwartz@fda.hhs.gov.

Registration: Registration is free and available on a first-come, first-served basis. Persons interested in attending this public workshop must register online by 4 p.m., October 14, 2014. Early registration is recommended because facilities are limited and, therefore, FDA may limit the number of participants from each organization. If time and space permit, onsite registration on the day of the public workshop will be provided beginning at 8:30 a.m.

If you need special accommodations due to a disability, please contact Susan Monahan, 301-796-5661, email: Susan.Monahan@fda.hhs.gov, no later than October 15, 2014.

To register for the public workshop, please visit FDA's Medical Devices News & Events--Workshops & Conferences calendar at http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/default.htm. (Select this public workshop from the posted events list.) Please provide complete contact information for each attendee, including name, title, affiliation, address, email, and telephone number. Those without Internet access should contact Suzanne Schwartz to register (see Contact Person). Registrants will receive confirmation after they have been accepted. You will be notified if you are on a waiting list.

Streaming Webcast of the Public Workshop: This public workshop will also be Webcast. Persons interested in viewing the Webcast must register online by 4 p.m., October 14, 2014. Early registration is recommended because Webcast connections are limited. Organizations are

requested to register all participants, but to view using one connection per location. Webcast participants will be sent technical system requirements after registration and will be sent connection access information after October 16, 2014. Most updated browsers will support the Webcast.

Comments: FDA is holding this public workshop to obtain information on medical device cybersecurity. In order to permit the widest possible opportunity to obtain public comment, FDA is soliciting either electronic or written comments on all aspects of the public workshop topics, regardless of attendance at the public workshop. The deadline for submitting comments related to this public workshop is November 24, 2014.

Regardless of attendance at the public workshop, interested persons may submit either electronic comments regarding this document to http://www.regulations.gov or written comments to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. It is only necessary to send one set of comments. Identify comments with the docket number found in brackets in the heading of this document. In addition, when responding to specific questions as outlined in section III of this document, please identify the question number you are addressing. Received comments may be seen in the Division of Dockets Management between 9 a.m. and 4 p.m., Monday through Friday, and will be posted to the docket at http://www.regulations.gov.

Transcripts: Please be advised that as soon as a transcript is available, it will be accessible at http://www.regulations.gov. It may be viewed at the Division of Dockets Management (see Comments). A transcript will also be available in either hardcopy or on CD-ROM, after submission of a Freedom of Information request. Written requests are to be sent to the Division of Freedom of Information (ELEM-1029), Food and Drug Administration, 12420 Parklawn Dr.,

Element Bldg., Rockville, MD 20857. A link to the transcripts will also be available approximately 45 days after the public workshop on the Internet at http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/default.htm. (Select this public workshop from the posted events list).

SUPPLEMENTARY INFORMATION:

I. Background

In February 2013, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," recognizing that resilient infrastructure is essential to preserving national security, economic stability, and public health and safety in the United States (Ref. 1). Executive Order 13636 states that cyber threats to national security are among the most serious, so stakeholders must enhance the cybersecurity and resilience of critical infrastructure. This includes the HPH Sector. Furthermore, Presidential Policy Directive (P.P.D.) 21 tasks Federal Government entities to strengthen the security and resilience of critical infrastructure against physical and cyber threats such that these efforts reduce vulnerabilities, minimize consequences, and identify and disrupt threats (Ref. 2). Moreover, P.P.D. 21 encourages all public and private owners and operators to share responsibility in achieving these outcomes. By convening this public meeting, FDA and its workshop partners strive to engage all stakeholders in HPH. These stakeholders include, but are not limited to: medical device manufacturers; healthcare facilities and personnel (e.g., healthcare providers, biomedical engineers, IT system administrators); professional and trade organizations (including medical device cybersecurity consortia); patient groups; insurance providers; cybersecurity researchers; local, State, and Federal Governments; and information security firms.

Executive Order 13636 and P.P.D. 21 together serve as a call to action for promoting the

cybersecurity of the Nation's critical infrastructure. The National Institute of Standards and Technology (NIST) developed the "Framework for Improving Critical Infrastructure Cybersecurity" ("Framework") with collective input from government agencies and the private sector to address Executive Order 13636's call for a voluntary, risk-based approach, harnessing a set of industry standards and best practices to manage cybersecurity risks (Ref. 3). P.P.D. 21 identifies critical sectors within the United States and charges each with adapting and implementing the Framework. HHS, as lead for the HPH Sector, seeks to adapt the Framework across its workspace. Developing a common lexicon is critical to this public-private collaboration to address and manage medical device cybersecurity risks. This workshop is an integral step towards the HPH Sector's collective understanding of the Framework and how it might be adapted to address the unique medical device cybersecurity needs and challenges within the sector.

If exploited, cyber vulnerabilities may result in medical device malfunction, disruption of healthcare services including treatment interventions, inappropriate access to patient information, or compromised electronic health record data integrity. Such outcomes could have a profound impact on patient care and safety. As devices become more connected and interoperable, the threat potential increases. Now, rather than impacting a single device or single system, multiple devices or an entire hospital network may be compromised. Addressing medical device cybersecurity requires recognizing interoperability and interconnectivity. Therefore, enhancing security and resilience entails designing healthcare systems for seamless integration. Such integration will foster innovative and interoperable medical devices that protect and improve patient health and safety.

Advancing medical device cybersecurity measures within the HPH Sector relies upon a

'whole of community' approach that will require acceptance of a 'shared ownership and shared responsibility' model. The objectives of such a model are twofold: (1) to seek solutions that incentivize businesses to adopt best practices and industry standards to be included in product design and systems architecture, and (2) to foster stakeholder collaboration such that emerging threat and vulnerability information is readily shared. This effort requires breaking down barriers and building trust between stakeholders. Ultimately, this effort will facilitate a forum to implement HPH cyber vulnerability and threat management.

II. Topics for Discussion at the Public Workshop

The public workshop sessions will incorporate the following general themes:

- Envisioning a collaborative environment for information sharing and developing a shared risk-assessment framework using a common lexicon;
- Overcoming barriers (perceived and real) to create a community of 'shared ownership and shared responsibility' within the HPH Sector to increase medical device cybersecurity;
- Gaining situational awareness of the current cyber threats to the HPH Sector, especially to medical devices;
- Identifying cybersecurity gaps and challenges, especially end-of-life support for legacy devices and interconnectivity of medical devices;
- Adapting and implementing the Framework to support management of cybersecurity risks involving medical devices;
- Developing tools and standards to build a comprehensive cybersecurity program to meet the unique needs of the sector's critical infrastructure, including medical devices;

- Leveraging the technical subject matter expertise of the cybersecurity researcher community working with HPH stakeholders to identify, assess, and mitigate vulnerabilities; and
- Building potential solutions: Exploring collaborative models to gather diverse experts and establish medical device security benchmarks which are continuously validated.

III. Questions for Consideration

FDA also requests HPH Sector stakeholders to provide perspective on the following:

1. Are stakeholders aware of the "Framework for Improving Critical Infrastructure Cybersecurity"? If so, how might we adapt/translate the Framework to meet the medical device cybersecurity needs of the HPH Sector?
2. How can we establish partnerships within the HPH Sector to quickly identify, analyze, communicate, and mitigate cyber threats and medical device security vulnerabilities?
3. How might the stakeholder community create incentives to encourage sharing information about medical device cyber threats and vulnerabilities?
4. What lessons learned, case studies, and best practices (from within and external to the sector) might incentivize innovation in medical device cybersecurity for the HPH Sector? What are the cybersecurity gaps from each stakeholder's perspective: knowledge, leadership, process, technology, risk management, or others? and,
5. How do HPH stakeholders strike the balance between the need to share health information and the need to restrict access to it?

The deadline for submitting answers to these questions for consideration and any other additional comments on the proposed workshop topics is October 7, 2014.

IV. References

1. Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," Feb. 19, 2013, available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
2. Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," Feb. 12, 2013, available at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
3. National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," version 1, Feb. 12, 2014, available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

Dated: September 17, 2014.

Leslie Kux,

Assistant Commissioner for Policy.

4164-01-P

[FR Doc. 2014-22515 Filed 09/22/2014 at 8:45 am; Publication Date: 09/23/2014]