4164-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

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

Moving Forward: Collaborative Approaches to Medical Device Cybersecurity; Public Workshop; Request for Comments

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice of public workshop; request for comments.

SUMMARY: The Food and Drug Administration (FDA) is announcing the following public workshop entitled "Moving Forward: Collaborative Approaches to Medical Device Cybersecurity." FDA, in collaboration with the National Health Information Sharing Analysis Center (NH-ISAC), the Department of Health and Human Services, and the Department of Homeland Security, seek to bring together diverse stakeholders to discuss complex challenges in medical device cybersecurity that impact the medical device ecosystem. The purpose of this workshop is to highlight past collaborative efforts; increase awareness of existing maturity models (i.e. frameworks leveraged for benchmarking an organization's processes) which are used to evaluate cybersecurity status, standards, and tools in development; and to engage the multi-stakeholder community in focused discussions on unresolved gaps and challenges that have hampered progress in advancing medical device cybersecurity.

DATES: The public workshop will be held January 20-21, 2016, from 9 a.m. to 5:30 p.m. Submit either electronic or written comments on the public workshop by February 22, 2016.

ADDRESSES: The public workshop will be held at the FDA White Oak Campus, 10903 New Hampshire Ave., Building 31 Conference Center, the Great Room, (rm. 1503), Silver Spring,

MD 20993-0002. Entrance for the public meeting participants (non-FDA employees) is through Building 1 where routine security check procedures will be performed. For parking and security information, please refer to http://www.fda.gov/AboutFDA/WorkingatFDA/BuildingsandFacilities/WhiteOakCampusInformation/ucm241740.htm.

You may submit comments as follows:

Electronic Submissions

Submit electronic comments in the following way:

- Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments. Comments submitted electronically, including attachments, to http://www.regulations.gov will be posted to the docket unchanged. Because your comment will be made public, you are solely responsible for ensuring that your comment does not include any confidential information that you or a third party may not wish to be posted, such as medical information, your or anyone else's Social Security number, or confidential business information, such as a manufacturing process. Please note that if you include your name, contact information, or other information that identifies you in the body of your comments, that information will be posted on http://www.regulations.gov.
- If you want to submit a comment with confidential information that you do not wish to be made available to the public, submit the comment as a written/paper submission and in the manner detailed (see "Written/Paper Submissions" and "Instructions").

Written/Paper Submissions

Submit written/paper submissions as follows:

- Mail/Hand delivery/Courier (for written/paper submissions): Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852.
- For written/paper comments submitted to the Division of Dockets Management, FDA will post your comment, as well as any attachments, except for information submitted, marked and identified, as confidential, if submitted as detailed in "Instructions."

Instructions: All submissions received must include the Docket No. FDA-2014-N-1286 for "Moving Forward: Collaborative Approaches to Medical Device Cybersecurity." Received comments will be placed in the docket and, except for those submitted as "Confidential Submissions," publicly viewable at http://www.regulations.gov or at the Division of Dockets Management between 9 a.m. and 4 p.m., Monday through Friday.

- Confidential Submissions--To submit a comment with confidential information that you do not wish to be made publicly available, submit your comments only as a written/paper submission. You should submit two copies total. One copy will include the information you claim to be confidential with a heading or cover note that states "THIS DOCUMENT CONTAINS CONFIDENTIAL INFORMATION". The Agency will review this copy, including the claimed confidential information, in its consideration of comments. The second copy, which will have the claimed confidential information redacted/blacked out, will be available for public viewing and posted on http://www.regulations.gov. Submit both copies to the Division of Dockets Management. If you do not wish your name and contact information to be made publicly available, you can provide this information on the cover sheet and not

in the body of your comments and you must identify this information as "confidential." Any information marked as "confidential" will not be disclosed except in accordance with 21 CFR 10.20 and other applicable disclosure law. For more information about FDA's posting of comments to public dockets, see 80 FR 56469, September 18, 2015, or access the information at: http://www.fda.gov/regulatoryinformation/dockets/default.htm.

Docket: For access to the docket to read background documents or the electronic and written/paper comments received, go to http://www.regulations.gov and insert the docket number, found in brackets in the heading of this document, into the "Search" box and follow the prompts and/or go to the Division of Dockets Management, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852.

FOR FURTHER INFORMATION CONTACT: Suzanne Schwartz, Food and Drug Administration, Center for Devices and Radiological Health, 10903 New Hampshire Ave., Bldg. 66, rm. 5428, Silver Spring, MD 20993, 301-796-6937, Suzanne.Schwartz@fda.hhs.gov.

SUPPLEMENTARY INFORMATION:

I. Background

Effective medical device cybersecurity to assure device safety and functionality has become more important with the increasing use of wireless, Internet- and network- connected devices, and the frequent electronic exchange of medical device-related health information. As medical devices become more connected and interoperable, the potential for exploit of device vulnerabilities, whether intentional or not, increases. Rather than impacting a single device or single system, multiple devices or an entire hospital network may be compromised. In the past, the Healthcare and Public Health (HPH) sector has been the target of many attempts at intrusion.

Protecting the HPH critical infrastructure from attack by strengthening cybersecurity is a high priority for the Federal government. Cybersecurity is the subject of recent Executive Orders focused on enhancing the cybersecurity of critical infrastructure (E.O. 13636) (Ref. 1) and increasing cybersecurity information sharing (E.O. 13691) (Ref. 2). Furthermore, Presidential Policy Directive 21 tasks the Federal government to work together with the private sector in order to strengthen the security and resilience of critical infrastructure against physical and cyber threats (Ref. 3). This public workshop will bring together diverse stakeholders from the public and private sector to discuss the current state of medical device cybersecurity, including its evolution over the past 12 months. Moreover, the workshop plans to provide a vision for the desired state of medical device cybersecurity through ongoing collaboration and new partnerships over the next 12 months. Meeting participants are encouraged to formulate strategies and feasible action plans to address gaps, such as management of vulnerabilities in legacy devices. These diverse 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.

A voluntary, risk-based framework for achieving enhanced cybersecurity was developed by the National Institute of Standards and Technology (NIST) in collaboration with external public and private sector partners (Ref. 4). Since its release in February 2014, the "Framework for Improving Critical Infrastructure Cybersecurity" (Framework) has been leveraged by entities within the HPH sector to better manage and reduce cybersecurity risks. This workshop aims to highlight some of the ways that the Framework has been employed to better understand, manage,

communicate, and mitigate medical device cybersecurity risks across the medical device total product lifecycle.

Medical device cybersecurity vulnerabilities, if exploited, may result in 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. In the last few years, HPH sector stakeholders have been engaged in many collaborative activities that seek to strengthen medical device cybersecurity and, therefore, enhance patient safety. FDA has contributed to these efforts through guidance, multi-stakeholder engagement, outreach, and by hosting a 2014 public workshop on cybersecurity (Ref. 5). The 2016 public workshop announced in this Federal Register notice will build upon previous work by featuring some of the collaborative efforts that address medical device cybersecurity through education and training, information sharing, standards, risk assessment, and tools development.

Though progress is evident, key hurdles continue to impede maturation of the HPH community's cybersecurity posture. This workshop seeks to increase awareness among stakeholders and create a common understanding of potential threats and vulnerabilities, as well as to present proactive preventative measures that may be universally employed as best practices and good cyber hygiene. The workshop also aims to facilitate extensive dialogue and articulate paths forward in the critical areas of information sharing, coordinated vulnerability disclosure and vulnerability management, and the Common Vulnerability Scoring System (CVSS). Information sharing continues to be a challenge as stakeholders work to define processes to create a trusted environment. Coordinated vulnerability disclosure is an important component of information sharing. Proactively identifying, assessing, and managing medical device

vulnerabilities before they are exploited is one way to protect against potential patient harm. Vulnerabilities may be identified by the device manufacturer as well as by external entities such as healthcare facilities, cybersecurity researchers, and other sectors of critical infrastructure. As described in International Organization for Standardization/International Electrotechnical Commission 29147:2014, "Coordinated disclosure, also known as responsible disclosure, is a vulnerability disclosure model in which all stakeholders agree to delay publishing vulnerability details for an agreed-upon period of time, generally after a patch to mitigate the vulnerability is available. The model includes steps that simplify the otherwise-complex, back-and-forth communications between the vulnerability finder and the affected manufacturer" (Ref. 6). Coordinated disclosure is just one aspect of vulnerability management. Understanding how a vulnerability may affect device functionality, assessing the vulnerability impact across multiple product types, and identifying mitigations that may be employed until a permanent fix may be implemented are all critical components of vulnerability management that should be addressed throughout the medical device total product lifecycle. This workshop provides an opportunity for stakeholders to explore implementation of coordinated vulnerability disclosure and vulnerability management, including existing standards, models, best practices, and lessons learned in this area.

One of the tools that manufacturers or healthcare facilities may use to assess and manage the impact of vulnerability is CVSS. CVSS is a risk assessment tool that provides an open and standardized method for rating information technology vulnerabilities. However, incorporating CVSS into medical device vulnerability assessments has proven to be a challenge in that it does not directly incorporate patient risk and public health impact factors. This workshop encourages robust dialogue on how CVSS might be adapted for medical devices and how considerations of

the use environment might be incorporated in a more standardized manner into medical device CVSS scores.

II. Topics for Discussion at the Public Workshop

The public workshop sessions are designed to incorporate the following general themes:

- Envisioning a roadmap for coordinated vulnerability disclosure and vulnerability management as part of the broader effort to create a trusted environment for information sharing.
    - How might the stakeholder community create incentives to encourage stakeholder participation?
    - What do individual stakeholders need to understand and be aware of regarding coordinated disclosure?
    - What current tools and models presently exist that may aid stakeholders in implementing disclosure and vulnerability management?
    - How can the security researcher community work in collaboration with HPH stakeholders to identify, assess, and mitigate vulnerabilities?
- Sharing FDA's current thinking on the implementation of the Framework in the medical device total product lifecycle.
- Adapting cybersecurity and/or risk assessment tools such as CVSS for the medical device operational environment.
- Adapting and/or implementing existing cybersecurity standards for medical devices.
- Understanding the challenges that manufacturers face as they increase collaboration with external third parties (cybersecurity researchers, Information Sharing and Analysis Organizations (ISAOs), and end users), to resolve cybersecurity vulnerabilities that

impact their devices. Note that an ISAO is a group created to gather, analyze, and disseminate critical infrastructure information (Ref. 7).

- Gaining situational awareness of the current activities in the HPH sector to enhance medical device cybersecurity.

- Identifying cybersecurity gaps and challenges that persist in the medical device ecosystem and begin crafting action plans to address them.

Registration: Registration is free and available on a first-come, first-served basis. Persons interested in attending this public workshop must register online by January 13, 2016, at 4 p.m. Early registration is recommended because facilities are limited and, therefore, FDA may limit the number of participants from each organization. If time and space permits, onsite registration on the day of the public workshop will be provided beginning at 8 a.m.

If you need special accommodations due to a disability, please contact Susan Monahan, Center for Devices and Radiological Health, Office of Communication and Education, 301-796-5661 or email: susan.monahan@fda.hhs.gov no later than January 7, 2016.

Please provide complete contact information for each attendee, including name, title, affiliation, email, and telephone number. Those without Internet access should contact Susan Monahan to register. 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. The Webcast link will be available on the registration Web page after January 13, 2016. Please visit FDA's Medical Devices News & Events--Workshops & Conferences calendar at http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/default.htm. Select this meeting/public workshop from the posted events list. If you have never attended a Connect

Pro event before, test your connection at https://collaboration.fda.gov/common/help/en/support/meeting_test.htm. To get a quick overview of the Connect Pro program, visit http://www.adobe.com/go/connectpro_overview. FDA has verified the Web site addresses in this document, but FDA is not responsible for any subsequent changes to the Web site after this document publishes in the Federal Register.

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 ADDRESSES). A transcript will also be available in either hardcopy or on CD-ROM, after submission of a Freedom of Information request. The Freedom of Information office address is available on the Agency's Web site at http://www.fda.gov. 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).

III. References

The following references are on display in the Division of Dockets Management (see ADDRESSES) and are available for viewing by interested persons between 9 a.m. and 4 p.m., Monday through Friday; they are also available electronically at http://www.regulations.gov. FDA has verified the Web site addresses, as of the date this document publishes in the Federal Register, but Web sites are subject to change over time.

1. Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 19, 2013 (http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf).

2. Executive Order 13691, “Promoting Private Sector Cybersecurity Information Sharing,” February 13, 2015 (http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf).
3. Presidential Policy Directive 21, “Critical Infrastructure Security and Resilience,” February 12, 2013 (http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil).
4. National Institute of Standards and Technology (NIST), “Framework for Improving Critical Infrastructure Cybersecurity,” version 1, February 12, 2014 (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf).
5. Food and Drug Administration, “Public Workshop -- Collaborative Approaches for Medical Device and Healthcare Cybersecurity, October 21-22, 2014.” October 11, 2015 (http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm412979.htm).
6. "ISO/IEC 29147:2014 -- Information Technology -- Security Techniques -- Vulnerability Disclosure," (http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170).
7. Department of Homeland Security, “Frequently Asked Questions About Information Sharing and Analysis Organizations (ISAOs),” November 17, 2015 (http://www.dhs.gov/isao-faq).

Dated: December 2, 2015.

Peter Lurie,

Associate Commissioner for Public Health Strategy and Analysis.

[FR Doc. 2015-30772 Filed: 12/4/2015 8:45 am; Publication Date: 12/7/2015]