4164-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. FDA-2015-D-5105]

Postmarket Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff; Availability

AGENCY: Food and Drug Administration, HHS

ACTION: Notice of availability.

SUMMARY: The Food and Drug Administration (FDA) is announcing the availability of a draft guidance entitled "Postmarket Management of Cybersecurity in Medical Devices." This draft guidance informs industry and FDA staff of the Agency's recommendations for identifying, addressing, and monitoring cybersecurity vulnerabilities and exploits for postmarket management of medical devices. This draft guidance is neither final nor is it in effect at this time.

DATES: Although you can comment on any guidance at any time (see 21 CFR 10.115(g)(5)), to ensure that the Agency considers your comment of this draft guidance before it begins work on the final version of the guidance, submit either electronic or written comments on the draft guidance by [INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: 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-2015-D- 5105 for "Postmarket Management of Cybersecurity in Medical Devices." 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.

Submit written requests for single copies of the guidance to the Office of the Center Director, Guidance and Policy Development, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5431, Silver Spring, MD 20993-0002 or the Office of Communication, Outreach, and Development, Center for Biologics Evaluation and Research, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 71, rm. 3128, Silver Spring, MD 20993-0002. Send one self-addressed adhesive label to assist that office in processing your requests. See the SUPPLEMENTARY INFORMATION section for electronic access to the draft guidance document.

FOR FURTHER INFORMATION CONTACT: Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5418, Silver Spring, MD 20993-0002, 301-796-6937; or Stephen Ripley, Center for Biologics Evaluation and Research, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 71, rm. 7301, Silver Spring, MD 20993-0002, 240-402-7911.

SUPPLEMENTARY INFORMATION:

I. Background

This draft guidance proposes to inform industry and FDA staff of the Agency's recommendations as it relates to monitoring, identifying, and addressing cybersecurity vulnerabilities and exploits as part of manufacturers' postmarket management of medical devices. A growing number of medical devices are designed to be networked to facilitate patient care. Networked medical devices, like other networked computer systems, incorporate software that may be vulnerable to cybersecurity threats. The exploitation of vulnerabilities may represent

a risk to the safety and effectiveness of medical devices and typically requires continual maintenance throughout the product life cycle to assure an adequate degree of protection against such exploits. Proactively addressing cybersecurity risks in medical devices reduces the patient safety impact and the overall risk to public health.

For the majority of cases, actions taken by manufacturers to address cybersecurity vulnerabilities and exploits are considered "cybersecurity routine updates and patches," for which the FDA does not require advance notification or reporting under 21 CFR part 806. For a small subset of cybersecurity vulnerabilities and exploits that may compromise the essential clinical performance of a device and present a reasonable probability of serious adverse health consequences or death, the FDA would require medical device manufacturers to notify the Agency.

In February 2013, the President issued Executive Order 13636 (E.O. 13636), "Improving Critical Infrastructure Cybersecurity," which recognized that resilient infrastructure is essential to preserving national security, economic stability, and public health and safety in the United States. Furthermore, Presidential Policy Directive-21 (PPD-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.

In addition, Executive Order 13691, released in February 2015, encourages the development of Information Sharing Analysis Organizations (ISAOs) to serve as focal points for cybersecurity information sharing and collaboration within the private sector and between the private sector and the government.

FDA believes that, in alignment with E.O. 13636 and PPD-21, stakeholders should collaborate to leverage available resources and tools to establish a common framework among the information technology community, healthcare delivery organizations (HDOs), clinical user community, and medical device community. These collaborations can lead to the consistent assessment and mitigation of cybersecurity threats, and their impact on medical device safety and effectiveness.

FDA plans to hold a public workshop entitled "Moving Forward: Collaborative Approaches to Medical Device Cybersecurity" on January 20-21, 2016 (80 FR 76022, December 7, 2015). FDA, in collaboration with the National Health Information Sharing Analysis Center, 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.

In the last few years, Healthcare and Public Health Critical Infrastructure 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, multistakeholder engagement, outreach, and by hosting a 2014 public workshop on cybersecurity entitled "Collaborative Approaches for Medical Device and Healthcare Cybersecurity" (79 FR 56814, September 23, 2014). The 2016 public workshop 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.

II. Significance of Guidance

This draft guidance is being issued consistent with FDA's good guidance practices regulation (21 CFR 10.115). The draft guidance, when finalized, will represent the Agency's current thinking on postmarket management of cybersecurity in medical devices. It neither creates nor confers any rights for or on any person and is not binding on FDA or the public. An alternative approach may be used if such approach satisfies the requirements of the applicable statutes and regulations.

III. Electronic Access

Persons interested in obtaining a copy of the draft guidance may do so by downloading an electronic copy from the Internet. A search capability for all Center for Devices and Radiological Health guidance documents is available at http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/default.htm. Guidance documents are also available at http://www.fda.gov/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/Guidances/default.htm or http://www.regulations.gov. Persons unable to download an electronic copy of "Postmarket Management of Cybersecurity in Medical Devices" may send an email request to CDRH-Guidance@fda.hhs.gov to receive an electronic copy of the document. Please use the document number 1400044 to identify the guidance you are requesting.

IV. Paperwork Reduction Act of 1995

This draft guidance refers to previously approved collections of information found in FDA regulations. These collections of information are subject to review by the Office of Management and Budget (OMB) under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3520). The collections of information in 21 CFR part 803 (medical device reporting) have been approved under OMB control number 0910-0437; the collections of information in 21 CFR part 806 (reports of corrections and removals) have been approved under OMB control number 0910-0359; the collections of information in 21 CFR part 810 (medical device recall authority) have been approved under OMB control number 0910-0432; the collections of information in 21 CFR part 814 (premarket approval) have been approved under OMB control number 0910-0231; the collections of information in 21 CFR part 820 (quality system regulations) have been approved under OMB control number 0910-0073; and the collections of information in 21 CFR part 822 (postmarket surveillance of medical devices) have been approved under OMB control number 0910-0449.

V. Other Issues for Consideration

The Agency invites comments on the "Postmarket Management of Cybersecurity in Medical Devices" draft guidance, in general, and on the following questions, in particular:

- What factors contribute to a manufacturer's decision whether or not to participate in an ISAO?
- In the draft guidance, the FDA is proposing its intention to not enforce certain regulatory requirements for manufacturer's that are "participating members " of an ISAO. Should FDA define what it means to be a "participating member" of an ISAO and if so, how should such participation be verified?

- What are the characteristics (participation, expertise, policies, and practices) of an ISAO that would make it qualified to participate in the sharing and analysis of medical device cybersecurity vulnerabilities? What are the benefits and disadvantages of FDA "recognizing" specific ISAOs as possessing specialized expertise relevant to sharing and analysis of medical device vulnerabilities and what should such recognition entail?
- When cybersecurity vulnerability information is not reported to FDA, what information should be reported to the ISAO, and when?
- How should the FDA interact with ISAOs, manufacturers, HDOs, security researchers and other stakeholders to maximize the sharing of information concerning cybersecurity threats while maintaining confidentiality and protecting commercial confidential information?

Dated: January 15, 2016.

Leslie Kux,

Associate Commissioner for Policy.

[FR Doc. 2016-01172 Filed: 1/21/2016 8:45 am; Publication Date: 1/22/2016]