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; Guidance for Industry and Food and Drug Administration; Availability

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice of availability.

SUMMARY: The Food and Drug Administration (FDA or Agency) is announcing the availability of the guidance entitled "Postmarket Management of Cybersecurity in Medical Devices." FDA is issuing this guidance to inform industry and FDA staff of the Agency's recommendations for managing postmarket cybersecurity vulnerabilities for marketed medical devices. The guidance clarifies FDA's postmarket recommendations with regards to addressing cybersecurity vulnerabilities and emphasizes that manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of the postmarket management of their medical devices.

DATES: Submit either electronic or written comments on this guidance at any time. General comments on Agency guidance documents are welcome at any time.

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.

An electronic copy of the guidance document is available for download from the Internet. See the SUPPLEMENTARY INFORMATION section for information on electronic access to the guidance. Submit written requests for a single hard copy of the guidance document entitled " "Postmarket Management of Cybersecurity in Medical Devices" 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 request.

FOR FURTHER INFORMATION CONTACT: Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, 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

On February 19, 2013, the President issued Executive Order 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. Executive Order 13636 states that cyber threats to national security are among the most

serious and that stakeholders must enhance the cybersecurity and resilience of critical infrastructure. This includes the Healthcare and Public Health Critical Infrastructure Sector. Furthermore, Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience (PPD-21) issued on February 12, 2013 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. PPD-21 encourages all public and private stakeholders to share responsibility in achieving these outcomes.

In recognition of the shared responsibility for cybersecurity, the security industry has established resources including standards, guidelines, best practices and frameworks for stakeholders to adopt a culture of cybersecurity risk management. Best practices include collaboratively assessing cybersecurity intelligence information for risks to device functionality and clinical risk. FDA believes that, in alignment with Executive Order 13636 and PPD-21, public and private stakeholders should collaborate to leverage available resources and tools to establish a common understanding that assesses risks for identified vulnerabilities in medical devices among the information technology community, healthcare delivery organizations, the clinical user community, and the 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, ultimately reducing potential risk of patient harm.

Part 806 (21 CFR part 806) requires device manufacturers or importers to report promptly to FDA certain actions concerning device corrections and removals. However, the majority of actions taken by manufacturers to address cybersecurity vulnerabilities and exploits, referred to as "cybersecurity routine updates and patches," are generally considered to be a type

of device enhancement for which the FDA does not require advance notification or reporting under part 806. For a small subset of actions taken by manufacturers to correct device cybersecurity vulnerabilities and exploits that may pose a risk to health, the FDA would require medical device manufacturers to notify the Agency.

This guidance clarifies changes to devices to be considered cybersecurity routine updates and patches (e.g., certain actions to maintain a controlled risk to health). In addition, the guidance outlines circumstances in which FDA does not intend to enforce reporting requirements under part 806 for specific vulnerabilities with uncontrolled risk. Specifically, FDA does not intend to enforce the reporting requirements when circumstances outlined in the guidance are met within the predefined periods of time (e.g., communicate vulnerability to customers and user community and propose a timeline for remediation within 30 days after learning of the vulnerability; fix the vulnerability and validate the change within 60 days after learning of the vulnerability; actively participate in an Information Sharing Analysis Organization (ISAO)). The Agency considers voluntary participation in an Information ISAO a critical component of a medical device manufacturer's comprehensive proactive approach to management of postmarket cybersecurity threats and vulnerabilities and a significant step towards assuring the ongoing safety and effectiveness of marketed medical devices.

II. Significance of Guidance

This guidance is being issued consistent with FDA's good guidance practices regulation (21 CFR 10.115). The guidance represents the current thinking of FDA on "Postmarket Management of Cybersecurity in Medical Devices." It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations.

III. Electronic Access

Persons interested in obtaining a copy of the 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 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 807, subpart E (premarket notification) have been approved under OMB control number 0910-0120; 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.

Dated: December 22, 2016.

Leslie Kux,

Associate Commissioner for Policy.

[FR Doc. 2016-31406 Filed: 12/27/2016 8:45 am; Publication Date: 12/28/2016]