RAPID7

Comments to FDA's Draft Guidance for Postmarket Management of Cybersecurity in Medical Devices

Docket Number: FDA-2015-D-5105

April 19, 2016

Rapid7 submits these comments in response to the U.S. Food and Drug Administration's (FDA)'s Draft Guidance for Postmarket Management of Cybersecurity in Medical Devices (draft guidance).[1] We appreciate that FDA issued this proactive and forward-looking draft guidance to address medical device cybersecurity.

Rapid7 is a cybersecurity analytics software and services company that helps organizations reduce the risk of a security breach, detect and investigate attacks, and build effective IT security programs. Identifying and addressing the vulnerabilities inherent in technical systems is a critical measure in mitigating cyber threats, reducing opportunities for attackers, and diminishing risks of harm to the victims of a security breach.

I. Holistic view of cybersecurity lifecycle, use of NIST Framework

The FDA draft postmarket guidance makes clear that cybersecurity risks extend throughout medical devices' lifecycle, and that cybersecurity risks cannot be totally eliminated before devices go to market.[2] At the same time, the draft guidance acknowledges that postmarket risk management does not substitute for a complete evaluation of premarket cybersecurity risks. Rapid7 strongly supports this holistic view of cybersecurity as beneficial to patients, other end-users, and businesses, and applauds FDA for formalizing this perspective in guidance. While premarket evaluation is a key and efficient means of controlling cyber threats, postmarket controls are critical to address evolving or overlooked vulnerabilities.

Rapid7 also believes FDA deserves credit for encouraging manufacturers to adopt the voluntary NIST Framework for Improving Critical Infrastructure Cybersecurity.[3] Rapid7 uses the Framework internally to inform our own security program and our product offerings, and externally to help clients build security programs. We believe the Framework is a pragmatic and modern approach to building a comprehensive cybersecurity program, and view increased industry and regulatory alignment with the Framework as positive.

II. Vulnerability disclosure

1) Company adoption of policy to receive vulnerabilities disclosed from third parties

[1] Notice of availability, Postmarket Management of Cybersecurity in Medical Devices, Draft Guidance for Industry and Food and Drug Administration Staff, 81 Fed. Reg. 3803-05, Jan. 22, 2016, https://www.federalregister.gov/articles/2016/01/22/2016-01172/postmarket-management-of-cybersecurity-in-medical-devices-draft-guidance-for-industry-and-food-and.

[2] Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices, Draft Guidance for Industry and Food and Drug Administration Staff, Jan. 22, 2016, Pg. 11, http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf.

[3] *Id.*, Pg. 6.

FDA's guidance lays out critical components of a cybersecurity risk management program.[4] One of these components is that a company adopt a coordinated vulnerability disclosure policy and practice. Rapid7 strongly supports the inclusion of this component. Even if companies do not pay researchers to find and disclose vulnerabilities ("bug bounty" programs), it is critical that companies have some means of receiving and processing vulnerabilities disclosed from external parties to keep their product security up to date. Organizations without such policies and practices face a greater probability of overlooking a vulnerability disclosure or responding inefficiently to a disclosure, putting patients at risk.

The draft guidance cites the ISO/IEC 29147:2014 standard for vulnerability disclosure.[5] We agree that the ISO standard is a good starting point for companies seeking to build a vulnerability disclosure policy. We suggest additionally noting that there may be other acceptable approaches for vulnerability disclosure,[6] as the draft guidance does elsewhere in referencing ANSI/AAMI/ISO 14971: 2007/(R)2010 with regard to assessing the impact of cybersecurity vulnerabilities on health.[7]

2) Vulnerability risk assessment

The draft guidance sets out two general categories of risk that cybersecurity vulnerabilities pose to essential clinical performance – controlled (acceptable) and uncontrolled (unacceptable). The draft guidance also provides a useful model for evaluating whether cybersecurity vulnerabilities are controlled or uncontrolled, measuring ease of exploitation and the severity of the health impact to patients if the vulnerability is exploited.[8] Manufacturers must notify FDA for uncontrolled vulnerabilities, but not necessarily for controlled vulnerabilities.[9] Rapid7 is supportive in concept of this approach, especially to the extent that the model can help prioritize vulnerabilities based on seriousness.

However, we are concerned that "essential clinical performance" is defined solely by the manufacturer.[10] Although FDA identifies a clear definition of essential clinical performance as a critical component of a cybersecurity risk management program, it is unclear when essential clinical performance must be defined and what specific factors FDA believes manufacturers should take into account when defining it. This increases the risk that manufacturers may establish a narrow definition of essential clinical performance, or create a definition in hindsight, that avoids reporting vulnerabilities to FDA.

The draft guidance is unclear on the extent to which a device vulnerability may have a serious impact on health and high exploitability, but can still fall outside the scope of a manufacturer's definition of essential clinical performance for that device. We recommend that the draft guidance make clear that high exploitability with serious impact on patient health should not be excluded from the definition of essential clinical performance. It would also be helpful for the draft guidance to note any check FDA has in place to prevent such scenarios.

Ideally, essential clinical performance would be defined in the premarket stage - once the definition is set, then any postmarket vulnerabilities can be measured against an established impact scale. In addition, if patients foreseeably use, whether intentionally or through error, devices in a manner that differs from the

[4] *Id.*, Pg. 11.
[5] *Id.*, Pg. 25.
[6] For example, Industrial Control Systems Cyber Emergency Response Team, ICS-CERT Vulnerability Disclosure Policy, https://ics-cert.us-cert.gov/ICS-CERT-Vulnerability-Disclosure-Policy (accessed Apr. 19, 2016).
[7] Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices, Draft Guidance for Industry and Food and Drug Administration Staff, Pg. 14.
[8] *Id.*, Pg. 15.
[9] *Id.*, Pgs. 17-18.
[10] *Id.*, Pg. 12.

manufacturers' intended use, manufacturers should incorporate that patient use as part of the definition of essential clinical performance. Rapid7 also recommends the draft guidance overtly support manufacturers working with trusted third party experts to assess device cybersecurity risks and vulnerabilities, especially when the manufacturer does not have adequate expertise or manpower on hand.[11] The draft guidance notes that postmarket cybersecurity information can originate from an array of sources, including independent researchers, but does not expressly encourage the use of trusted third parties where appropriate.[12]

III. Vulnerability mitigation

It is positive that the draft guidance notes that patching devices post market is a combined effort among multiple stakeholders, including companies not necessarily regulated by FDA.[13] Many foundational elements of medical device software rely on libraries and packages supplied by commercial off-the-shelf software (OTS). Vulnerabilities that affect OTS can therefore undermine the security of medical devices using the OTS. FDA discusses these issues in its 2005 Guidance for Industry Cybersecurity for Networked Medical Devices Containing Off-the-Self (OTS) Software,[14] but the problem is still prevalent.[15] It would be helpful if this draft guidance on postmarket considerations expressly recommended that manufacturers work closely with OTS vendors to eliminate vulnerabilities rooted in the OTS.

The draft guidance's description of "cybersecurity routine updates and patches" notes that routine patches include regularly scheduled updates to a device, but exclude updates to patch vulnerabilities with a reasonable probability of serious health consequences.[16] This issue is further complicated when the underlying OTS is no longer supported by the original vendor, creating greater risk that a serious vulnerability will go unpatched. It would be helpful if the draft guidance provided more detail with regard to the responsibilities of manufacturers for notifying FDA or patients when a vulnerability that would severely impact patient health is present in the OTS.

Rapid7 believes it is critical for medical products to have a robust security update mechanism wherever feasible. Although draft guidance refers to updates in several places, does not specifically encourage update mechanisms as part of a comprehensive risk management program. [17] We suggest revising the list of critical components of a comprehensive cybersecurity risk management program to include update mechanisms where feasible. It is positive that the draft guidance notes conditions under which patches and updates need not be reported to FDA, to reduce instances in which vendors believe FDA processes hinder issuance of the update.[18]

[11] See for example, discussion of FCC Recognized Testing Laboratories. Federal Communications Commission, Equipment Authorization, Approval Guide, https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization (accessed Apr. 19, 2016).

[12] Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices, Draft Guidance for Industry and Food and Drug Administration Staff, Pg. 12.

[13] *Id.*, Pg. 5.

[14] Food and Drug Administration, Guidance for Industry, Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, Jan. 14, 2005, http://www.fda.gov/RegulatoryInformation/Guidances/ucm077812.htm.

[15] Rene Millman, *Nearly 1,500 vulnerabilities found in automated medical equipment*, SC Magazine, Mar. 31, 2016, http://www.scmagazine.com/nearly-1500-vulnerabilities-found-in-automated-medical-equipment/article/486497.

[16] Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices, Draft Guidance for Industry and Food and Drug Administration Staff, Pg. 8.

[17] *Id.*, Pg. 12.

[18] *Id.*, Pg. 18.

IV. Enforcement

Rapid7 recognizes that this is a guidance document with non-binding recommendations. Although we applaud and support FDA's proactive approach to addressing postmarket cybersecurity in this draft guidance, we would support enforceable standards for postmarket device cybersecurity that go beyond Federal Trade Commission authority, including converting these draft guidelines into required activities. Establishing enforceable postmarket cybersecurity standards would be a complex undertaking involving many stakeholders, but we believe such standards would ultimately provide greater protection to patients' health.

*   *   *

We appreciate the opportunity to share our views. If there are additional questions or if Rapid7 can provide any further assistance, please contact Harley Geiger, Rapid7 Director of Public Policy, at Harley_Geiger@Rapid7.com. Thank you.

END