ALSTON&BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTONPRIVACY.COM OCTOBER 10, 2014

FDA Issues Final Cybersecurity Guidance

By Kim Peretti and Cathy Burgess
Contributors: Lou Dennig and Brendan Carroll

On October 2, 2014, the U.S. Food and Drug Administration (FDA) took another critical step towards mitigating and managing cybersecurity threats by releasing a Final Guidance, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (the Guidance).[1] The Guidance urges manufacturers of medical devices to consider cybersecurity risks when designing and developing their medical devices. Although FDA lays out recommendations to manufacturers in the Guidance to aid them in managing cybersecurity risks and protecting patient health information, there is no indication that specific devices or systems have been targeted. The Guidance serves as a vehicle for FDA to raise concerns about device-related cybersecurity vulnerabilities and their potential for adverse impacts on public health.

Cybersecurity vulnerabilities create risks for the safe and effective operation of network-connected medical devices or computers, smartphones and tablets used to access patient data. Because the loss or theft of sensitive patient information places patient safety at risk, manufacturers are faced with the challenge of addressing cybersecurity threats and mitigating patients' risks while promoting the development of innovative medical devices and improving device functionality.

The Guidance contains many of the recommendations that FDA introduced in its Draft Guidance issued in June 2013. Note, however, that the Guidance contains new recommendations that demonstrate FDA's sophistication in cybersecurity developments. For example, FDA chose to use terminology from the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the "Framework").[2] Released in February of this year, months after FDA issued its Draft Guidance, the Framework was developed in response to an Executive Order[3] President Obama issued to

---

1 See "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff," (October 2, 2014), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.

2 *See* National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure," *available at*: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

3 *See* Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11739, *available at*: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

improve the cybersecurity capabilities of the nation's critical infrastructure. The Framework is designed as a guide for companies to use in developing cybersecurity policies and practices. It organizes such practices into five "Core Functions:" Identify, Protect, Detect, Respond and Recover. In the Guidance, FDA used those Core Functions to organize the cybersecurity practices it believes device manufacturers should adopt. While the actual recommended protections are nearly identical in both the Draft and Final Guidance, by viewing those protections through the lens of the Framework, FDA underscored the government's commitment to push further adoption and use of the Final Guidance. Such efforts are gaining traction, as this past week Commerce Department General Counsel Kelly Welsh stated that his department has seen "expanding networks" of organizations leverage the Framework in developing their cybersecurity practices.[4]

The Guidance also includes recommendations for the type of cybersecurity documentation companies should include in their premarket submissions, all of which are predicated on effective design controls that are implemented and managed as part of a company's quality system. In addition to hazard analysis, mitigations and design considerations related to intentional and unintentional cybersecurity risks, FDA advises companies to include a traceability matrix that demonstrates the relationship between the cybersecurity controls implemented and the cybersecurity risks that were contemplated. Two additional requirements that FDA altered slightly in the Guidance include a summary describing the plan for providing validated updates and patches to the operating system or software throughout the life cycle of the device as well as a summary describing controls that ensure both the integrity of the device and that it remains free of malware. Finally, FDA requires manufacturers to include appropriate device instructions for product use. The documentation about the controls companies have in place, including ongoing software patches and updates to operating systems, is intended to mitigate the threat of hackers accessing their devices.

Although FDA presents the information contained in the Guidance as "recommendations" for use by medical device manufacturers, these "recommendations" will ultimately serve as important guidelines for companies to follow as they design and develop new devices. Unsophisticated companies, and those that do not have the proper expertise within the company, that fail to take into account appropriate cybersecurity concerns from the beginning may encounter problems with their premarket submissions, ultimately resulting in the inability to obtain 510(k) clearance or premarket approval.[5] If cybersecurity concerns are not addressed in the premarket submission, FDA may require the submission of additional information, resulting in multiple rounds of review.

---

4 *See* "U.S. Cybersecurity Framework Touted as 'Valuable' Legal Tool," *BNA Bloomberg* (Oct. 1, 2014), *available at*: http://privacylaw.bna.com/pvrc/7060/split_display.adp?fedfid=57024126&vname=prabulallissues&jd=a0f6u0z4k2&split=0.

5 The Guidance applies to the following premarket submissions for medical devices: premarket notification (510(k)) including Traditional, Special and Abbreviated), *de novo* submissions, premarket approval applications (PMA), product development protocols (PDP) and humanitarian device exemption (HDE) submissions. *See* Guidance at 2.

The increased scrutiny will undoubtedly come from FDA's new cybersecurity lab, the launch of which was announced in June 2013 with the release of the Draft Guidance. In August 2013, FDA awarded the contract for the laboratory to Codenomicon Defensics,[6] which works with FDA to conduct "fuzz testing," an automated robustness testing system designed to most efficiently detect unknown vulnerabilities in medical devices. During this testing, medical devices are fed invalid, unexpected or random data that can be used to detect stability issues within the coding of the device. It appears FDA will integrate fuzz testing capabilities into its cybersecurity labs, but it remains to be seen what FDA will do with manufacturers whose devices fail these tests. Nonetheless, FDA's partnership with industry to develop medical technology cyber standards represents a new barrier to market that companies will need to consider. The key to compliance with the requirements set forth in the Guidance will be to contemplate cybersecurity at the early stages of medical device design and development.

In conjunction with the release of the Guidance, FDA also announced it is planning a public workshop October 21-22 in Arlington, VA to discuss how government, medical device developers, hospitals, cybersecurity professionals and other stakeholders can collaborate to improve the cybersecurity of medical devices and protect the public health. The meeting is being held in collaboration with the Department of Homeland Security to address the issue of medical device cybersecurity, which is quickly being recognized as a serious vulnerability associated with emerging health care technology.

FDA continues to consider and recognize the importance of cybersecurity issues related to medical devices, and finalizing this important Guidance signals FDA's intention to institute a more robust regulatory oversight of medical devices to ensure that cybersecurity risks are minimized to the greatest extent possible. With the help of Codenomicon Defensics, FDA's new cybersecurity laboratory will undoubtedly prove to be a critical component to the testing and oversight of medical devices and may even present a challenging barrier to market entry for some companies. Companies seeking to design and develop medical devices within FDA's framework will need to contemplate these important recommendations in their daily operations.

Security Incident Management & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

---

6 See "Codenomicon Defensics – Fuzz Testing Software," Solicitation Number: FDA-13-1120705 (July 21, 2013), *available at* https://www.fbo.gov/index?s=opportunity&mode=form&id=579ab0f9fbf869ffe2cebb605fec27a2&tab=core&_cview=0.