INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

June 28, 2013

Division of Dockets Management (HFA–305)
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

Dear Sirs/Madam:

Re: Comments for Content of Premarket Submissions for Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff (HFA-305 / Docket No. FDA–2013–D–0616)

On behalf of the Chair of the Information Security and Privacy Advisory Board (ISPAB or Board), Matt Thomlinson, I would like to submit the attached letter as the Board's comments for the draft guidance entitled "*Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*."

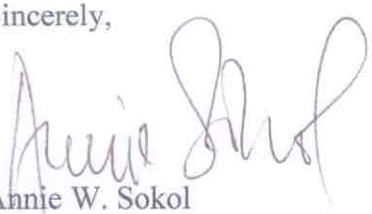
The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-235) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002. The statutory objectives of the Board include identifying emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

The letter was the Board's recommendation to US Office of Management and Budget, Washington, DC, based on a panel discussion conducted at the Board's meeting, February 1-3, 2012. The letter signed by immediate past Chair, Dan Chenok, includes observations and findings from the panel discussion, and recommendations, that the Board considers as appropriate comments in response to the draft guidance.

Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-2938 *** Fax: 301/975-4007

In addition to the attached recommendation letter, information on the discussion and panelists can be found from ISPAB's web site
http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/february-2012.html

Sincerely,



Annie W. Sokol
Designated Federal Officer
Information Security and Privacy Advisory Board
IT Specialist, NIST

Attachment – ISPAB Letter on medical devices

cc. ISPAB

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

March 30, 2012

The Honorable Jeffrey Zients
Acting Director, US Office of Management and Budget
Washington, DC 20502

Dear Mr. Zients,

I am writing to you as the Chair of the Information Security and Privacy Advisory Board (ISPAB or Board). The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-35) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002. One of the statutory objectives of the Board is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

At the Board meeting of February 1-3, 2012, the Board discussed the issue of maintaining security in medical devices that are increasingly operated by software connected to the public Internet, possibly through wireless connections. The Board heard experts discuss how lack of cybersecurity preparedness for millions of software-controlled medical devices puts patients at significant risk of harm. Specifically, software-controlled medical devices are increasingly available through and exposed to cybersecurity risks on the Internet; examples range from desktop computers controlling radiological imaging to custom embedded software found in pacemakers. With increasing connectivity comes greater functionality and manageability, but also increased risks of both unintentional interference and malicious tampering via these communication channels.

Further complicating this picture, the economics of medical device cybersecurity involves a complex system of payments between multiple stakeholders -- including manufacturers, providers, and patients. At the same time, no one agency has primary responsibility from Congress to ensure the cybersecurity of medical devices deployed across this spectrum;

Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-2938 *** Fax: 301/975-4007

agencies involved include Centers for Medicare and Medicaid Services (CMS) and Food and Drug Administration (FDA) in Department of Health and Human Services (HHS), as well as the Department of Defense (DOD), Department of Veterans' Affairs (VA), and Department of Homeland Security (DHS), among others. Given the complexity of the technical issues involved, the Board finds that diffusion of responsibility when it comes to cybersecurity of medical devices raises growing concern.

In addition, there is an economic disincentive for reporting of vulnerabilities and incidents – a hospital, for example, can incur liability by reporting a problem. A lack of meaningful data on medical device cybersecurity can lead to cybersecurity unpreparedness because cybersecurity problems that go unreported can increase a false impression of preparedness due to lower incident counts. This lack of reported incidents also results from a lack of effective reporting mechanisms from clinical settings to the Government about cybersecurity threats in medical devices.

The Board made the following observations from the panel discussion:

- There is a diffusion of Government responsibility for cybersecurity of medical devices, leading to lack of accountability and oversight.

- Current medical device reporting methods, primarily captured through FDA, are not designed to capture indicators of medical device cybersecurity problems.

- Medical devices used in the home raise additional cybersecurity risks, given the less trustworthy nature of the home environment.

- The Government has multiple ways to address cybersecurity for medical devices, including regulation through FDA, purchasing power through CMS, information distribution through numerous agencies, and education and awareness to home users and medical providers.

Based on the Board's discussion and findings, we offer a number of recommendations:

1. A single Federal entity (such as FDA) should be assigned responsibility for taking medical device cybersecurity into account during pre-market clearance and approval of devices, and during post-market surveillance of cybersecurity threat indicators at time of use.

2. FDA should collaborate with National Institute of Standards and Technology (NIST) scientists and engineers to research cybersecurity features that could be enabled by default on networked or wireless medical devices in Federal settings. For instance, a

medical provider should not have to download new software, such as an anti-virus product, to achieve an acceptable baseline of cybersecurity. Cybersecurity features in medical devices should be active at the time of purchase by the Government, and should be easily and transparently configurable by a provider at the time of use; this can translate into improved cybersecurity in device acquisition across a broad spectrum of buyers.

3. The Government should assign a lead entity (such as Health Resources and Services Administration (HRSA) or FDA in HHS) to establish better training and education that informs users, health care organizations, and manufacturers about the risks associated with networked and wireless medical devices. This lead organization should make information readily available to all parties upon receipt of a medical device, as well as part of the "instructions for use" for the users.

4. Because medical devices are increasingly Internet-based, United States Computer Emergency Readiness Team (US-CERT) should create defined reporting categories for medical device cybersecurity incidents. Coordination is necessary with US-CERT to establish mechanisms that incentivize Government, providers, and manufacturers to collect cybersecurity threat indicators so that the country is prepared for the inevitable growth in device incident reports.

5. Further study is needed to determine whether additional policy or legislative changes are necessary to promote medical device security.

The Board appreciates the opportunity to provide views on this emerging and important issue. We welcome further discussion at the Administration's discretion.

Sincerely,

Daniel J. Chenok
Chair, ISPAB

cc: The Honorable Kathleen Sebelius, Secretary, Department of Health and Human Services
Steven VanRoekel, Administrator of E-Government and Information Technology and CIO, OMB
Howard Schmidt, Cybersecurity Coordinator, National Security Council,
Mark Weatherford, Deputy Undersecretary for Cybersecurity, DHS
Patrick Gallagher, Director, NIST

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. FDA–2013–D–0616]

Content of Premarket Submissions for 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.

SUMMARY: The Food and Drug Administration (FDA) is announcing the availability of the draft guidance entitled ''Content of Premarket Submissions for Management of Cybersecurity in Medical Devices.'' This guidance identifies cybersecurity issues that manufacturers should consider in preparing premarket submissions for medical devices in order to maintain information confidentiality, integrity, and availability. This draft guidance is not 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 on 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 September 12, 2013.

ADDRESSES: Submit written requests for single copies of the draft guidance document entitled ''Content of Premarket Submissions for Management of Cybersecurity in Medical Devices'' to the Division of Small Manufacturers, International, and Consumer Assistance, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, Rm. 4613, Silver Spring, MD 20993–0002 or the Office of Communication, Outreach and Development (HFM–40), 1401 Rockville Pike, Suite 200N, Rockville, MD 20852. Send one self-addressed adhesive label to assist that office in processing your request, or fax your request to 301–847–8149. See the **SUPPLEMENTARY INFORMATION** section for information on electronic access to the guidance.

Submit electronic comments on the draft guidance to *http://www.regulations.gov.* Submit written comments to the Division of Dockets Management (HFA–305), Food and Drug Administration, 5630 Fishers Lane, Rm. 1061, Rockville, MD 20852. Identify comments with the docket number found in brackets in the heading of this document.

FOR FURTHER INFORMATION CONTACT: Abiy Desta, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, Rm. 1682, Silver Spring, MD 20993–0002, 301–796–0293, *Abiy.Desta@fda.hhs.gov;* or Stephen Ripley, Center for Biologics Evaluation and Research (HFM–17), Food and Drug Administration, 1401 Rockville Pike, Suite 200N, Rockville, MD 20852, 301–827–6210.

SUPPLEMENTARY INFORMATION:

I. Background

This draft guidance provides recommendations to consider and document in FDA medical device premarket submissions to provide effective cybersecurity management and to reduce the risk that device functionality is intentionally or unintentionally compromised. The need for effective cybersecurity to assure medical device 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.

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 management of cybersecurity in medical devices. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public. An alternative approach may be used if such approach satisfies the requirements of the applicable statute and regulations.

III. Electronic Access

Persons interested in obtaining a copy of the draft guidance may do so by using 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.regulations.gov* or from the Center for Biologics Evaluation and Research at *http://www.fda.gov/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/default.htm.* To receive ''Content of Premarket Submissions for Management of Cybersecurity in Medical Devices,'' you may either send an email request to *dsmica@fda.hhs.gov* to receive an electronic copy of the document or send a fax request to 301–847–8149 to receive a hard copy. Please use the document number 1825 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 807, subpart E, have been approved under OMB control number 0910–0120; the collections of information in 21 CFR part 812 have been approved under OMB control number 0910–0078; the collections of information in 21 CFR part 814 have been approved under OMB control number 0910–0231; the collections of information in 21 CFR part 814, subpart H, have been approved under OMB control number 0910–0332; and the collections of information in 21 CFR part 820 have been approved under OMB control number 0910–0073.

V. Comments

Interested persons may submit either electronic comments regarding this document to *http://www.regulations.gov* or written comments to the Division of Dockets Management (see **ADDRESSES**). It is only necessary to send one set of comments. Identify comments with the docket number found in brackets in the heading of this document. Received comments may be seen in the Division of Dockets Management between 9 a.m. and 4 p.m., Monday through Friday, and will be posted to the docket at *http://www.regulations.gov.*

Dated: June 11, 2013.

Leslie Kux,

Assistant Commissioner for Policy.

[FR Doc. 2013–14167 Filed 6–13–13; 8:45 am]

BILLING CODE 4160–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. FDA–2010–D–0616]

Guidance for Industry on Codevelopment of Two or More New Investigational Drugs for Use in Combination; Availability

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice.

SUMMARY: The FDA is announcing the availability of a guidance for industry entitled ''Codevelopment of Two or More New Investigational Drugs for Use