JAMES R. LANGEVIN
2D DISTRICT, RHODE ISLAND

COMMITTEE ON ARMED SERVICES
EMERGING THREATS AND CAPABILITIES
(RANKING)
SEAPOWER AND PROJECTION FORCES

COMMITTEE ON
HOMELAND SECURITY
CYBERSECURITY, INFRASTRUCTURE
PROTECTION, AND SECURITY TECHNOLOGIES

Congress of the United States
House of Representatives
Washington, DC 20515–3902

WASHINGTON OFFICE:
109 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
TELEPHONE: (202) 225–2735
FAX: (202) 225–5976

DISTRICT OFFICE:
THE SUMMIT SOUTH
300 CENTERVILLE ROAD, SUITE 200
WARWICK, RI 02886
TELEPHONE: (401) 732–9400
FAX: (401) 737–2982

http://langevin.house.gov

April 21, 2016

Dr. Suzanne Schwartz
Director Emergency Preparedness/Operations and Medical Countermeasures
c/o Division of Dockets Management (HFA-305)
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

Re: Docket No. FDA-2015-D-5105 - Postmarket Management of Cybersecurity in Medical Devices

Dear Dr. Schwartz:

Thank you for the opportunity to comment on the Food and Drug Administration's proposed guidance FDA-2015-D-5105, regarding postmarket management of cybersecurity in medical devices. I write as a Member of Congress with an abiding interest in cybersecurity, particularly within the critical infrastructure sectors as identified by Presidential Policy Directive 21. I strongly support FDA's efforts to improve the security of medical devices, and if finalized, the draft guidance would make substantial progress in this area.

The spread of enhanced communications abilities to medical devices has the potential to bring great benefits to patients. Being able to wirelessly monitor settings in a pacemaker, for instance, allows for doctors to check-in on patients without requiring a trip to the office. Thanks to network connectivity, other medical devices can be diagnosed or reprogrammed more efficiently and can collect more data to allow care providers to furnish individualized treatments.

However, like other tools joining the growing constellation of objects that are part of the Internet of Things, medical devices are subject to increased risk as their connectivity grows. Some of this risk is a result of growing complexity of the systems: more lines of code mean more opportunity for error. Much of the risk, though, derives from a greater possibility of intentional misuse of systems. Where once accessing a medical device required specialized equipment or physical presence, today a malicious user can potentially connect from anywhere. This is a paradigmatic change in what it means for a device to be "safe," and the postmarket guidance is an important step in adapting the regulatory environment to this new reality.

The postmarket guidance should prove particularly effective due to its emphasis on risk-based cybersecurity. Like any security domain, cybersecurity is not binary: there is no perfectly secure system. In assessing cybersecurity activities, device manufacturers must weigh the aims of the threat actors and the degree of vulnerability in the system with the impact on patients. The postmarket guidance captures two of these dimensions, addressing the degree of exploitability and the severity of impact to health of discovered vulnerabilities. Given the difficulty of tracking the many threat actors in the space, this focus is appropriate.

The risk-based nature of the guidance extends to the recommended cybersecurity practices medical device manufacturers should adopt. Rather than outline specific controls, which would rapidly become obsolete, the guidance suggests processes, such as monitoring cybersecurity information sources, that are tied to a holistic model of risk. Of note are the recommendations regarding vulnerability handling and disclosure, as effective vulnerability programs are essential for alerting manufacturers to security problems.

The guidance also wisely makes use of a voluntary approach to remediating and reporting cybersecurity flaws in medical devices. As FDA points out, manufacturers are already required to report devices representing an uncontrolled risk to essential clinical performance under 21 CFR part 806, whether the risk is due to a software vulnerability or some other reason. By stating willingness to forebear enforcing these requirements, FDA provides an incentive for manufacturers to adopt measures including a thirty day remediation timeline and membership in an Information Sharing and Analysis Organization. The guidance clearly contemplates the difficulties that can arise in pushing a software patch within a short time frame by allowing for compensating controls. Swift remediation, notification of customers, and participation in information sharing represent the heart of the guidance and are well tuned to materially improve patient safety within the industry.

Beyond promulgating this guidance, FDA has an important responsibility to ensure that manufacturers are properly complying with the proposed mitigation methods or are properly reporting cybersecurity risks under 21 CFR part 806. I encourage FDA to build upon its successful collaborations with industry in this space as exemplified by the cybersecurity workshops begun in 2014. By working together with manufacturers, caregivers, patients, information technology experts, and security researchers, FDA can build a safer environment that still allows for innovations around medical device networking.

Thank you again for the opportunity to comment on this important issue. I again commend FDA for its proactive involvement with cybersecurity policy and for its work with stakeholders in developing the postmarket guidance. If you have any questions regarding the submittal, please contact my office at (202) 225-2735.

Sincerely,

JAMES R. LANGEVIN
Member of Congress