DIANA DEGETTE
1ST DISTRICT, COLORADO

2335 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-4431
FAX (202) 225-5657

DISTRICT OFFICE:
600 GRANT STREET, SUITE 202
DENVER, CO 80203
(303) 844-4988
FAX (303)844-4996

http://degette.house.gov

Congress of the United States
House of Representatives
Washington, DC 20515-4329

CHIEF DEPUTY WHIP
COMMITTEE ON ENERGY AND COMMERCE
RANKING MEMBER
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
SUBCOMMITTEE ON ENVIRONMENT AND THE ECONOMY
SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

November 3, 2016

Robert M. Califf, M.D.
Commissioner
U.S. Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

Jeffrey Shuren, M.D., J.D.
Director, Center for Devices and Radiological Health
U.S. Food and Drug Administration
10903 New Hampshire Avenue
WO66-5429
Silver Spring, MD 20993

Dear Commissioner Califf and Director Shuren,

We write to seek more information from FDA about potential cybersecurity vulnerabilities in medical devices. As the Internet of Things (IoT) proliferates, so too does the number of networked medical devices. Numerous devices, ranging from monitors and infusion pumps, to ventilators and radiological technologies, are integrated into the nation's digitized healthcare network, creating possible avenues for cyber-attacks.

While the risks to patients may be low today, approximately 10 to 15 million medical devices in circulation across the United States use technologies that could be susceptible to cyber-attacks. This is especially important due to the rapidly evolving pace of cyber threats, as many of these existing devices are more than 10 years old and when designed could have never anticipated the current cyber threat landscape. Individual medical devices could also potentially serve as an entry point for bad actors to use ransomware against healthcare providers, thus not only putting a single patient at risk, but jeopardizing the operations of entire health systems.

We know medical device manufacturers are working closely with the U.S. Food and Drug Administration (FDA), security researchers, and other stakeholders to ensure that all potential vulnerabilities are addressed. We applaud FDA and other stakeholders for the steps that have already been taken to protect patients against potential emerging threats. Nevertheless, we have also seen recent headlines about the potential for unauthorized access in insulin pumps and implantable cardiac devices, among others. While innovative networked systems and the growth of wireless technology broaden the reach and effectiveness of lifesaving devices, they also increase the risk of cyber criminals taking advantage of technology's inherent weaknesses. As technology will undoubtedly continue to evolve at a rapid pace, we must ensure that FDA is equipped with the appropriate cybersecurity expertise and resources to evaluate not only the current risks to new medical devices, but also how new threats affect the medical devices already in use.

We are pleased FDA has identified mitigating medical device cybersecurity vulnerabilities as a regulatory science priority in 2017.[1] We also appreciate FDA's guidance in October 2014 on managing cybersecurity issues in

[1] U.S. Food and Drug Administration Center for Device and Radiological Health Regulatory Science Priorities (FY2017)

premarket submissions and draft guidance in January 2016 on postmarket cybersecurity management. As FDA encounters more complex issues and sophisticated devices, we would like to know more about how the Agency is working to prevent emerging threats, mitigate existing vulnerabilities, and assess the strength of a device's cyber resilience.

- What steps is FDA taking to notify device manufacturers and the provider community that cybersecurity vulnerability mitigation is a priority?

- How is the FDA working with medical device manufacturers and other stakeholders to assist them in protecting against potential vulnerabilities and emerging cybersecurity threats in both premarket and postmarket contexts?

- How is FDA working with medical device manufactures to ensure that known vulnerabilities to individual patients and/or entire health systems are mitigated and disclosed to all users? What efforts are currently underway to ensure that providers and patients are properly informed about known vulnerabilities among devices currently deployed for patient care?

- What is FDA doing to ensure that network owners, such as hospitals, implement practices and policies to keep their systems and connected devices secure?

- Given the potentially long lifecycle of some devices, what is the FDA doing to ensure that device security and patient privacy is accounted for throughout the prolonged use of devices despite the emergence of new threat vectors?

- Does the Agency have the personnel, policies and infrastructure necessary to evaluate how a device's security capabilities relate to the safety and efficacy of the device's functionality?

- How is the Agency coordinating its cybersecurity initiatives with other agencies, both within the Department of Health and Human Services (HHS), and across the federal government, including the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI) and the Federal Trade Commission (FTC)?

Thank you for your attention to this important matter. We look forward to collaborating with FDA, device manufacturers, and other stakeholders to ensure that the nation's patients have access to safe and secure medical devices. We respectfully request a response from the Agency by December 16, 2016.

Sincerely,

Diana DeGette
Member of Congress

Susan W. Brooks
Member of Congress

Cc: Representative Fred Upton, Chairman, House Energy & Commerce Committee
Representative Frank Pallone Jr., Ranking Member, House Energy & Commerce Committee