United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510–6275

November 9, 2018

VIA ELECTRONIC TRANSMISSION

The Honorable Scott Gottlieb, M.D.
Commissioner
U.S. Food & Drug Administration

Dear Commissioner Gottlieb,

The Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21), tasked Federal entities with strengthening the security and resiliency of critical infrastructure against physical and cyber threats.[1] The Department of Health and Human Services was designated to oversee the health care and public health sectors in this regard.[2] In 2017, the Health Care Industry Cybersecurity Task Force identified as an "imperative" the need to "increase the security and resilience of medical devices and health IT" in order to keep patients safe and protect their information from vulnerability or exploitation.[3] Cyber risks to the health care sector are real, ongoing, and all reasonable efforts must be taken to combat them to protect patients.

On November 1, 2018, the Department of Health and Human Services Office of Inspector General released a report outlining some deficiencies in the Food and Drug Administration's (FDA) regulation and oversight of post market medical device cybersecurity.[4] The FDA is responsible for ensuring the safety and effectiveness of medical devices. While I applaud the proactive steps the FDA took during the course of the drafting of the report to improve medical device cybersecurity, I am writing to ensure that this progress continues and that any remaining deficiencies are fixed.

The report highlighted some very important issues where the FDA has room for improvement. Specifically, the OIG stated that the FDA's "plans and processes were deficient in

[1] Presidential Policy Directive, Critical Infrastructure Security and Resilience, February 12, 2013. Available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[2] *Id.*
[3] HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE, REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY, 28 (2017). Available at https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.
[4] Naomi Thomas, *FDA isn't doing enough to prevent medical device hacking, HHS report says*, CNN, Nov. 1, 2018, https://www.cnn.com/2018/11/01/health/fda-unprepared-medical-device-hacking/index html.

addressing medical device cybersecurity compromises."[5] OIG found that there was a lack of adequate testing of FDA's ability to respond to medical device cybersecurity events, and two of its district offices had no written standard operating procedures to address recalls of medical devices that were vulnerable to cyber-attacks.[6] OIG recommended four action items, including the establishment of written procedures and practices for securely sharing sensitive information about cybersecurity events with stakeholders and entering into formal agreements with federal partners to support FDA's cybersecurity mission.[7] According to the report, the FDA disagreed with OIG's conclusions that the lack of a formal agreement with federal partners impedes information flow about cybersecurity incidents and that it had failed to properly assess medical device cybersecurity at an enterprise or component level.[8] Despite this, OIG maintained that "FDA's efforts to address medical device cybersecurity vulnerabilities were susceptible to inefficiencies, unintentional delays, and potentially insufficient analysis."[9]

These revelations are particularly troubling because it is clear that foreign governments have focused on our governmental systems to leverage them for their benefit.[10] For example, I recently wrote a letter to NIH raising concerns about foreign governments effectively installing foreign agents in U.S. based research institutions to steal intellectual property produced by taxpayer funded studies.[11] Medical devices could be exploited by those same foreign actors to not only interfere with normal device operation, which could cause harm to patients, but also to steal personal medical information. I think you can agree, action must be taken to reduce and eliminate these threats.

Additionally, the FDA's website states that every year, the FDA receives hundreds of thousands of reports through medical device reporting (MDR) pertaining to device-related malfunctions, serious injuries, and deaths.[12] It's important that Congress gain a better understanding of what the FDA does with MDR data.

Accordingly, please provide written responses to the following questions no later than November 23, 2018:

1. With respect to each of the four OIG recommendations, please provide the Committee a written summary, on a rolling basis if necessary, describing how the FDA implemented fixes sufficient to close the recommendations.[13]

---

[5] DEP'T OF HEALTH AND HUMAN SERV., OFFICE OF INSPECTOR GEN., REPORT NO. A-18-16-30530, THE FOOD AND DRUG ADMINISTRATION'S POLICIES AND PROCEDURES SHOULD BETTER ADDRESS POSTMARKET CYBERSECURITY RISK TO MEDICAL DEVICES, Report in Brief (2018). Available at https://oig hhs.gov/oas/reports/region18/181630530.pdf.
[6] *Id.*
[7] *Id.* at 12-13.
[8] *Id.* at 13.
[9] *Id.* at 7-8.
[10] *See, e.g.*, Letter from Hon. Charles E. Grassley, Chairman, Senate Judiciary Comm., to Hon. Francis Collins, Director, National Institute of Health (October 23, 2018); Letter from Hon. Charles E. Grassley, Chairman, Senate Judiciary Comm., to Hon. Jeff Sessions, Attorney General, U.S. Department of Justice (September 19, 2018).
[11] Letter to National Institute of Health, *supra* n. 10.
[12] U.S. Food & Drug Admin., Medical Device Reporting (MDR) Overview (last updated on Sept. 25, 2018). Accessed at https://www.fda.gov/medicaldevices/safety/reportaproblem/default.htm on November 7, 2018.
[13] DEP'T OF HEALTH AND HUMAN SERV., OFFICE OF INSPECTOR GENERAL, *supra* note 5, at 12-13.

2. Has the FDA assessed whether foreign governments or other entities are threats to post market medical device cybersecurity? If so, which governments or entities has FDA identified?

3. With respect to MDR data reports, please answer the following:

    a. Please explain how the FDA is using MDR data.
    b. Is this data being used to improve cybersecurity for medical devices?
    c. Can the MDR system be utilized to report cybersecurity concerns?

4. Please provide a briefing to my Committee staff regarding cyber security threats to medical devices and the steps FDA is taking to combat them.

I anticipate that your written reply and most responsive documents will be unclassified. Please send all unclassified material directly to the Committee. In keeping with the requirements of Executive Order 13526, if any of the responsive documents do contain classified information, please segregate all unclassified material within the classified documents, provide all unclassified information directly to the Committee, and provide a classified addendum to the Office of Senate Security. Although the Committee complies with all laws and regulations governing the handling of classified information, it is not bound, absent its prior agreement, by any handling restrictions.

Thank you in advance for your prompt attention to these matters. Should you have any questions, please contact Josh Flynn-Brown of my Committee staff at (202) 224-5225.

Sincerely,

Charles E. Grassley
Chairman
Committee on the Judiciary