Report in Brief
Date: October 2018
Report No. A-18-16-30530

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

Why OIG Did This Review

We conducted this audit because OIG had identified ensuring the safety and effectiveness of medical devices and fostering a culture of cybersecurity as top management challenges for HHS. We also considered public and Congressional interest in medical device cybersecurity risks to patients and the Internet of Things. The Food and Drug Administration (FDA) is the HHS operating division responsible for assuring that legally marketed medical devices are safe and effective.

Our objective was to determine the effectiveness of FDA's plans and processes for timely communicating and addressing cybersecurity medical device compromises in the postmarket phase.

How OIG Did This Review

We focused this audit on FDA's internal processes for addressing the cybersecurity of medical devices in the postmarket phase. To accomplish our objective, we reviewed FDA's policies, procedures, manuals, and guides; interviewed staff; and reviewed publicly available information on FDA's website. We also analyzed FDA's processes for receiving and evaluating information on medical device compromises. In addition, we tested the internal controls at FDA's Center for Devices and Radiological Health to determine whether they ensured an effective response to a medical device cybersecurity incident.

The Food and Drug Administration's Policies and Procedures Should Better Address Postmarket Cybersecurity Risk to Medical Devices

What OIG Found

FDA had plans and processes for addressing certain medical device problems in the postmarket phase, but its plans and processes were deficient for addressing medical device cybersecurity compromises. Specifically, FDA's policies and procedures were insufficient for handling postmarket medical device cybersecurity events; FDA had not adequately tested its ability to respond to emergencies resulting from cybersecurity events in medical devices; and, in 2 of 19 district offices, FDA had not established written standard operating procedures to address recalls of medical devices vulnerable to cyber threats.

These weaknesses existed because, at the time of our fieldwork, FDA had not sufficiently assessed medical device cybersecurity, an emerging risk to public health and to FDA's mission, as part of an enterprise risk management process. We shared our preliminary findings with FDA in advance of issuing our draft report. Before we issued our draft report, FDA implemented some of our recommendations. Accordingly, we kept our original findings in the report, but, in some instances, removed our recommendations.

What OIG Recommends and FDA Comments

We recommend that FDA do the following: (1) continually assess the cybersecurity risks to medical devices and update, as appropriate, its plans and strategies; (2) establish written procedures and practices for securely sharing sensitive information about cybersecurity events with key stakeholders who have a “need to know”; (3) enter into a formal agreement with Federal agency partners, namely the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team, establishing roles and responsibilities as well as the support those agencies will provide to further FDA's mission related to medical device cybersecurity; and (4) ensure the establishment and maintenance of procedures for handling recalls of medical devices vulnerable to cybersecurity threats.

FDA agreed with our recommendations and said it had already implemented many of them during the audit and would continue working to implement the recommendations in the report. However, FDA disagreed with our conclusions that it had not assessed medical device cybersecurity at an enterprise or component level and that its preexisting policies and procedures were insufficient. We appreciate the efforts FDA has taken and plans to take in response to our findings and recommendations, but we maintain that our findings and recommendations are valid.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/181630530.asp.