Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

THE FOOD AND DRUG ADMINISTRATION'S POLICIES AND PROCEDURES SHOULD BETTER ADDRESS POSTMARKET CYBERSECURITY RISK TO MEDICAL DEVICES

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Gloria L. Jarmon
Deputy Inspector General
for Audit Services

October 2018
A-18-16-30530

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC

at https://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG website.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

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

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

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

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.

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.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS REVIEW

We conducted this audit because the Office of Inspector General (OIG) had identified ensuring the safety and effectiveness of medical devices and fostering a culture of cybersecurity as top management challenges for the Department of Health and Human Services (HHS). We conducted extensive preliminary research and held discussions with external medical device experts to understand the postmarket cybersecurity risks with medical devices.

We also considered public and Congressional interest in the Internet of Things,[1] as well as medical device cybersecurity risks to patients. In 2016, the House Energy and Commerce Committee held a hearing, "Understanding the role of connected devices in recent cyberattacks." That hearing reviewed a series of device-based denial-of-service attacks and considered future efforts to respond to the targeting of vulnerabilities in infrastructure, including medical devices. In addition, on December 30, 2016, the Internet of Things Working Group,[2] co-chaired by Representatives Bob Latta and Peter Welch, published its "Year-End White Paper" that, in part, discussed how the Internet of Things improves patient care yet presents many challenges. The paper stated, "participants in the healthcare sector view data protection, cybersecurity, and privacy as top concerns and priorities."

The Food and Drug Administration (FDA) is the HHS operating division responsible for ensuring there is a reasonable assurance of the safety and effectiveness of medical devices.

OBJECTIVE

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

[1] One description of "Internet of Things" is "the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems." Accessed at https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf) on April 6, 2018.

[2] According to the White Paper, "The goals of our working group are to educate members on the Internet of Things (IoT), identify issues affecting deployment of these emerging technologies, explore the benefits and challenges of the IoT for consumers and interested stakeholders, examine the possible role of the federal government in advancing IoT technologies, and explore the potential for public-private partnerships in this sector." Accessed at https://latta.house.gov/uploadedfiles/iot_working_group_white_paper.pdf on April 6, 2018.

BACKGROUND

Federal Oversight of Cybersecurity

Executive Order No. 13636, issued on February 12, 2013, recognized that cyber threats continue to grow as one of the most serious threats to national security and that resilient critical infrastructure is essential to preserving national security, economic stability, and public health and safety in the United States.[3,4] The Department of Homeland Security (DHS) leads the Federal Government's efforts to secure our Nation's critical infrastructure. Critical infrastructure includes products marketed by companies from the health care and public health sectors, including medical device manufacturers. The order supported the enhancement of the security and resilience of the Nation's critical infrastructure, and a cyber environment that encourages efficiency, innovation, and economic prosperity. The order also supported an increase in the volume, timeliness, and quality of cyber threat information that Federal entities share with the private sector. Executive Order No. 13800, issued on May 11, 2017, also stated that it is the policy of the executive branch to support the cybersecurity of our Nation's critical infrastructure.[5]

The Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21), issued on February 12, 2013, tasked Federal entities with strengthening the security and resiliency of critical infrastructure against physical and cyber threats in an effort to reduce vulnerabilities, minimize consequences, and identify and disrupt threats.[6] This responsibility included working with the private sector to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure. HHS was designated as the Federal agency with the institutional knowledge and specialized expertise to oversee the health care and public health sectors.[7] HHS is responsible for managing the response to incidents in the health care and public health sectors, as well as providing, supporting, and facilitating technical assistance and consultation to identify vulnerabilities and help mitigate incidents.

[3] Executive Order No. 13636, published at 78 Fed. Reg. 11739 (Feb. 19, 2013).

[4] Executive Order No. 13636 defines "critical infrastructure" to mean systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

[5] Executive Order No. 13800, published at 82 Fed. Reg. 22391 (May 16, 2017).

[6] Presidential Policy Directive 21, February 12, 2013. Accessed at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil on April 6, 2018.

[7] PPD-21 also designated USDA and HHS as co-sector-specific agencies to oversee the Food and Agriculture Sector.

Executive Order No. 13800 instructed the sector-specific agencies to engage the owners and operators of critical infrastructure and identify ways the Federal Government can support their cybersecurity efforts. In 2017, the Health Care Industry Cybersecurity Task Force identified increasing the security and resilience of medical devices and health information technology (IT) as an imperative that must be achieved to increase security within the health care industry.[8]

FDA and Its Oversight of Medical Devices

To increase effectiveness and ultimately improve patient care, some medical devices may connect to the Internet, hospital or other networks, and other medical devices. Innovative advancements offer new promise and new risks, as medical devices have become more vulnerable to cybersecurity vulnerabilities, exploitations, and threats that may affect their safety and effectiveness.

Under the Federal Food, Drug, and Cosmetic Act (FD&C Act), it is FDA's mission to ensure there is a reasonable assurance that medical devices legally marketed in the United States are safe and effective for their intended uses.[9] FDA's Center for Devices and Radiological Health (CDRH) develops and carries out a national program to ensure that patients and providers have access to safe and effective medical devices. CDRH is responsible for regulating firms that design, manufacture, repackage, relabel, or import medical devices sold in the United States.

FDA regulates medical devices using a "total product lifecycle" approach, which consists of two phases: premarket and postmarket.[10] In the premarket phase, FDA assesses whether a medical device is safe and effective for its intended use. To receive FDA clearance or approval to market a medical device in the United States, a manufacturer must submit to FDA proper documentation showing that its device is safe and effective. In the postmarket phase—after FDA clears or approves a medical device—FDA conducts oversight activities, such as monitoring and investigating the medical device's safety and effectiveness, and alerting the public of problems when warranted.[11] Postmarket requirements for medical device manufacturers include the tracking and reporting of device malfunctions, serious injuries, and deaths; reporting corrections and removals; registering establishments; and compliance with quality system regulation.

---

[8] Health Care Industry Task Force, *Report on Improving Cybersecurity in the Health Care Industry* (June 2017). Accessed at https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf on April 13, 2017.

[9] FD&C Act § 1003.

[10] FDA Fact Sheet, "FDA's Role in Medical Device Cybersecurity,". Accessed at https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf on April 6, 2018.

[11] FDA, *The Device Development Process, Step 5: FDA Post-Market Device Safety Monitoring*, January 2018. Accessed at https://www.fda.gov/ForPatients/Approvals/Devices/ucm405428.htm on October 19, 2018.

FDA's Oversight of Medical Device Cybersecurity in the Postmarket Phase

In alignment with Executive Order No. 13636 and PPD-21, FDA's ongoing efforts to protect the public health from cybersecurity events include conducting public workshops and webinars; entering into Memoranda of Understanding with the National Health Information Sharing and Analysis Center and the Medical Device Innovation, Safety, and Security Consortium; and issuing product-specific safety communications that discuss cybersecurity vulnerabilities.

In 2013, FDA's CDRH and its Center for Biologics Evaluation and Research formed the Cybersecurity Workgroup. The workgroup is charged with defining and evolving FDA's thinking about its oversight of medical device cybersecurity. This task includes working with the medical device industry and other stakeholders and formulating policies and guidance on medical device cybersecurity. The workgroup is composed of FDA subject matter experts and senior FDA staff. The workgroup is not intended to routinely provide technical consultation for specific device issues; rather, the workgroup is intended to leverage information from individual device issues to inform broader policy frameworks and agency guidance. These policies and practices are intended to help ensure the safety and effectiveness of marketed medical devices in the United States.[12]

Manufacturers are responsible for ensuring the ongoing safety and performance of marketed medical devices.[13] This responsibility includes validating the design of the device in the premarket phase, which must include testing under actual or simulated use conditions.[14] According to FDA guidance, in the postmarket phase manufacturers should remain vigilant and monitor, identify, and address cybersecurity vulnerabilities and threats.[15] FDA guidance also states that manufacturers are responsible for validating design changes through testing in the postmarket phase, including software changes to address cybersecurity vulnerabilities and threats.[16] To help manage postmarket cybersecurity vulnerabilities, FDA encourages manufacturers to participate in Information Sharing and Analysis Organizations.[17] In

[12] FDA, CDRH Cybersecurity Workgroup Charter, Version 1.1 (June 6, 2017).

[13] 21 CFR § 820.100.

[14] FDA, Guidance for Industry and FDA Staff, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (Oct. 2014). Accessed at https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf on April 13, 2018.

[15] FDA, Guidance for Industry and FDA Staff, *Postmarket Management of Cybersecurity in Medical Devices* (Dec. 2016). Accessed at https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf on April 6, 2018.

[16] *Id*.

[17] Executive Order No. 13691 encouraged the development of Information Sharing and Analysis Organizations.

December 2016, FDA issued guidance entitled "Guidance for Industry and FDA Staff, Postmarket Management of Cybersecurity in Medical Devices." The intent of the guidance was to inform FDA staff and the public, including Information Sharing and Analysis Organizations, of its recommendations for managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices.

In addition to issuing guidance, FDA continues to address myths about medical device cybersecurity and published a fact sheet entitled "The FDA's Role in Medical Device Cybersecurity, Dispelling Myths and Understanding Facts."[18] In the fact sheet, FDA clarified it is a myth that "[t]he FDA tests medical devices for cybersecurity." It is fact that "[t]he FDA does not conduct premarket testing for medical products. Testing is the responsibility of the medical product manufacturer." FDA's fact sheet also states it is myth that "[t]he FDA is responsible for the validation of software changes made to address cybersecurity vulnerabilities." [19] It is fact that "[t]he medical device manufacturer is responsible for the validation of all software design changes, including computer software changes to address cybersecurity vulnerabilities."

Sometimes medical device manufacturers learn that there are problems with their medical devices. Manufacturers and others must report to FDA certain device usage problems and corrections.[20] For example, a manufacturer may be required to report to FDA the distribution of a patch to fix a cybersecurity vulnerability that could cause a life-threatening injury. If a device is defective or a risk to public health, a manufacturer may voluntarily recall[21] the device. FDA oversees voluntary recalls to ensure effectiveness and, in consultation with the recalling firm, makes information about the recall publicly available.[22] If FDA becomes aware of a firm that refuses to voluntarily recall its device, FDA may order it to conduct a recall if there is a reasonable probability that the device will cause serious, adverse health consequences or death.[23] The FDA district office responsible for overseeing the region where a recalling firm is located is designated as the lead district and is responsible for providing guidance to the recalling firm and monitoring day-to-day recall activities.[24]

---

[18] Accessed at https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf on April 6, 2018.

[19] *Id.*

[20] FD&C Act § 360i.

[21] FDA uses the term "recall" when a manufacturer takes a correction or removal action to address a problem with a medical device that violates the FD&C Act. "Correction" means the repair, modification, adjustment, relabeling, destruction, or inspection of a product without its physical removal to some other location (21 CFR § 7.3).

[22] 21 CFR part 7.

[23] FD&C Act § 360h(e) and 21 CFR part 810.

[24] In 2017, FDA's Office of Regulatory Affairs (ORA) implemented a program-based management structure that aligns staff by FDA-regulated product and replaced its management structure based on geographic regions.

Emergencies involving medical devices also have the potential to cause adverse health and safety effects, and CDRH participates in FDA's emergency preparedness and response efforts.

Management's Responsibility for Assessing Risk and Establishing Internal Control

Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, issued July 15, 2016, provides guidance to Federal managers and defines management's responsibilities for enterprise risk management (ERM) and internal control. The circular emphasizes the need to integrate and coordinate risk management and strong and effective internal controls into existing business activities and as an integral part of managing an agency. The circular states:

> Each Federal employee is responsible for safeguarding Federal assets and the efficient delivery of services to the public. Federal leaders and managers are responsible for establishing goals and objectives around operating environments, ensuring compliance with relevant laws and regulations, and managing both expected and unexpected or unanticipated events. They are responsible for implementing management practices that identify, assess, respond, and report on risks. Risk management practices must be forward-looking and designed to help leaders make better decisions, alleviate threats and to identify previously unknown opportunities to improve the efficiency and effectiveness of government operations. Management is also responsible for establishing and maintaining internal controls to achieve specific internal control objectives related to operations, reporting, and compliance.

OMB Circular No. A-123 also establishes an assessment framework based on the Government Accountability Office's *Standards for Internal Control in the Federal Government* (The Green Book) that managers must integrate into risk management and internal control functions.

HOW WE CONDUCTED THIS REVIEW

OIG's Office of Evaluation and Inspections conducted a study of FDA's oversight of medical device cybersecurity during the premarket phase entitled *FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Review Process for Medical Devices*.[25] OIG's Office of Audit Services focused our audit on the internal processes FDA has in place to address medical device cybersecurity in the postmarket phase. To accomplish our objective, we reviewed FDA's policies, procedures, manuals, and guides; interviewed staff; and reviewed public information available on FDA's website. We also analyzed FDA's processes for receiving and evaluating information on medical device compromises. In addition, we tested CDRH's

[25] OIG report OEI-09-16-00220, issued on September 10, 2018. Accessed at https://oig.hhs.gov/oei/reports/oei-09-16-00220.asp on October 9, 2018.

internal controls to determine whether they ensured an effective response to a medical device cybersecurity incident.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions. We communicated to FDA our preliminary findings in advance of issuing our draft report.

Appendix A describes our audit scope and methodology; Appendix B contains Federal requirements and guidance for enterprise risk management[26] and internal controls; and Appendix C contains excerpts from the "FDA Fact Sheet, The FDA's Role in Medical Device Cybersecurity, Dispelling Myths and Understanding Facts."

FINDINGS

FDA had plans and processes for addressing certain medical device problems in the postmarket phase (e.g., defects, malfunctions, unsafe designs), but its plans and processes were deficient in addressing medical device cybersecurity compromises. Specifically:

- FDA's policies and procedures had not adequately addressed handling postmarket medical device cybersecurity events.

- FDA had not adequately tested its ability to respond to emergencies resulting from cybersecurity events in medical devices.

- FDA had not established written standard operating procedures (SOPs) that address recalls of medical devices vulnerable to cyber threats in 2 of 19 district offices.

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 FDA's mission, as part of an enterprise risk management process.

We did not identify evidence that FDA mismanaged or responded untimely to a reported medical device cybersecurity event. However, because FDA had not sufficiently assessed the risks of medical device cybersecurity events, existing policies and procedures did not include effective practices for responding to those events. Therefore, FDA's efforts to address medical

[26] According to OMB Circular No. A-123, "ERM is an effective Agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provides better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery."

device cybersecurity vulnerabilities were susceptible to inefficiencies, unintentional delays, and potentially insufficient analysis.

After we concluded our fieldwork, but before we issued our report, FDA provided us with evidence supporting its implementation of some of our preliminary recommendations. We continue to report our findings as identified, but we added language to the findings briefly describing the actions FDA had taken to address our findings. In some instances, we removed our recommendations. We appreciate FDA's proactive steps to address our findings.

FDA'S POLICIES AND PROCEDURES HAD NOT ADEQUATELY ADDRESSED HANDLING POSTMARKET MEDICAL DEVICE CYBERSECURITY EVENTS

Medical device cybersecurity events are an emerging risk to public health and FDA's mission. According to OMB Circular No. A-123, the identification of risk is a continuous and ongoing process, must be forward thinking, and must be regularly reviewed.

FDA staff from the Emergency Operations Program and the CDRH Cybersecurity Workgroup manage FDA's response to medical device cybersecurity events. CDRH has processes for receiving information from manufacturers, hospitals, and others about medical device usage problems, such as deaths and serious injuries related to the use of medical devices, medical device malfunctions, product quality problems, and product use errors. However, since the inception of the Cybersecurity Workgroup in 2013, FDA had not developed and implemented procedures to ensure the Cybersecurity Workgroup efficiently receives and shares information about cybersecurity vulnerabilities, exploits, and threats that potentially affect medical devices. Specifically:

- FDA had not established group email accounts or electronic mailboxes for the Cybersecurity Workgroup to receive information about cybersecurity vulnerabilities, exploits, and threats, although it had established group email accounts and electronic mailboxes for receiving medical device complaints and information about device safety issues within other CDRH offices.

- FDA had not developed a resource, such as an online application or form, for the Cybersecurity Workgroup to receive cybersecurity threat, vulnerability, and exploit information on medical devices from certain external users.

- FDA had not defined a method for the Cybersecurity Workgroup to securely share proprietary or other sensitive information associated with medical device cybersecurity vulnerabilities, exploits, and threats with stakeholders outside FDA.

- FDA had not formalized the Cybersecurity Workgroup's ability to receive or share medical device cybersecurity vulnerability information from or with other Federal

agencies, including DHS and the Department of Energy's Idaho National Laboratory.[27] FDA had also not assessed risks related to CDRH's collaboration, management, and information sharing of cybersecurity vulnerabilities or coordinated response actions with DHS. FDA officials informed us that the Cybersecurity Workgroup has an informal two-way relationship with the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) whereby the Cybersecurity Workgroup may become aware of a vulnerability and share its findings with DHS. Conversely, DHS may become aware of a vulnerability and share its findings with FDA. DHS may also legitimize specific device vulnerabilities[28] that security researchers, manufacturers, or hospitals bring to CDRH's attention.

We also identified specific weaknesses with the CDRH SOP entitled *Triaging Incidents or Potential Emergency Events with CDRH* (Triaging SOP). The Triaging SOP outlines CDRH's processes for triaging, tracking, and managing emergency events.[29] CDRH employees also use the Triaging SOP to determine whether an event is an emergency. The Triaging SOP:

- did not clearly define "emergency" to include a cybersecurity threat, vulnerability, or exploit in medical devices[30] and

- did not correctly list the appropriate points of contact for Emergency Operations Program personnel.[31]

[27] The Department of Energy's Idaho National Laboratory conducts research related to securing critical infrastructure and reducing cyber vulnerabilities.

[28] Examples include buffer overflow, improper input validation, hard-coded passwords, and improper authentication. Buffer overflow is a condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated. Improper input validation occurs when the product does not validate or incorrectly validates input that can affect the control flow or data flow of a program. "Hard-coded passwords" is a term for putting nonencrypted (plain text) passwords and other secret data (such as private keys) into the source code. Improper authentication occurs when the software does not adequately prove a user's identity.

[29] CDRH, Standard Operating Procedure on Triaging Incidents or Potential Emergency Events within CDRH, Version 1.3, effective June 16, 2014.

[30] The Triaging SOP defined an emergency as "an urgent need for health care [medical] services to respond to a disaster, significant outbreak of an infectious disease, bioterrorist attack, or other significant or catastrophic event and demands decision-making and follow-up in terms of extraordinary measures. An emergency may involve the safety, efficacy, and security of human and veterinary medicines, biological products, medical devices, our Nation's food supply, cosmetics, products that emit radiation, or tobacco products, and call for immediate actions by FDA staff."

[31] The Emergency Operations Program personnel are responsible for monitoring an event's progress and coordinating efforts across multiple offices within CDRH or with organizations outside of CDRH.

Inadequacies in FDA's policies and procedures existed because, at the time of our fieldwork, FDA:

- had not assessed medical device cybersecurity risk at an enterprise or component level;
- had not established a charter to formalize the CDRH Cybersecurity Workgroup; and
- had not assessed risks related to CDRH's collaboration, management, and information sharing of cybersecurity vulnerabilities or coordinated response actions with DHS.

As a result, FDA put at risk the effectiveness of its strategy to leverage existing procedures for handling cybersecurity events in medical devices and its ability to effectively and efficiently receive, evaluate, and track medical device cybersecurity vulnerabilities, exploitations, and threats.

After we concluded our fieldwork, but before we issued our report, FDA provided documentation supporting its first assessment of enterprise risk, which included cybersecurity risk to medical devices. FDA also provided us with an SOP entitled *EMCM Cybersecurity Signal Management* that describes CDRH's process for receiving, tracking, and fielding cybersecurity signals, and it instructs the Emergency Operations Program staff to share certain information about specific medical device vulnerabilities and exploits with the Cybersecurity Workgroup when appropriate.[32] Additionally, FDA provided us with a charter for the Cybersecurity Workgroup dated June 6, 2017. The charter defined the purpose of the Cybersecurity Workgroup as promoting "the development and implementation of policies and practices pertaining to FDA's review and oversight of medical device cybersecurity." It also defined the workgroup's scope, goals, metrics, roles, responsibilities, and organization structure. Lastly, FDA provided us with an updated Triaging SOP that updated the definition of "emergency" to include certain compromises resulting from an exploitation of a cybersecurity vulnerability.[33] Accordingly, we have no recommendations for FDA to develop a charter for the CDRH Cybersecurity Workgroup or to update its Triaging SOP.

[32] CDRH, Standard Operating Procedure on EMCM Cybersecurity Signal Management, Version 1.0, effective December 13, 2017.

[33] CDRH, Standard Operating Procedure on Triaging Incidents or Potential Emergency Events within CDRH, Version 2.0, effective December 13, 2017.

FDA HAD NOT ADEQUATELY TESTED ITS ABILITY TO RESPOND TO EMERGENCIES RESULTING FROM CYBERSECURITY EVENTS IN MEDICAL DEVICES

The National Institute of Standards and Technology recommends that organizations have IT plans in place so that they can effectively respond to and manage adverse situations.[34] It is important for personnel to be trained to fulfill their roles and responsibilities, to conduct exercises to validate policies and procedures, and to test systems to ensure operability. This methodology can be applied to any type of IT-related plan, including disaster recovery plans and computer security incident response plans.

FDA's Emergency Operations Plan (EOP) is intended to be used as a guide in conducting response operations for all types of incidents. The EOP states that FDA will conduct tests, training, and exercises to ensure agency personnel are familiar with assigned emergency roles and responsibilities.[35]

FDA did participate in two response and recovery exercises, but the exercises did not involve cybersecurity events affecting medical devices. The first response and recovery exercise in July 2015 involved a nuclear power plant incident as part of a Federal Emergency Management Agency Radiological Emergency Preparedness Program exercise. The second response and recovery exercise in March 2016 was for cyberattacks targeting several critical infrastructure sectors as part of DHS's national-level cyber exercise.

FDA documented the following lessons learned from the March 2016 exercise:

- nothing in the exercise involved the potential for patient harm;
- a medical device sector-specific exercise would be beneficial;
- the DHS Industrial Control Systems Cyber Emergency Response Team staff with whom FDA normally engaged and typically coordinated with in the event of a cyber-response were not active participants in the exercise;
- FDA and HHS should have a thorough understanding of, among other things, departmental capabilities, roles and responsibilities, and communication mechanisms as they relate to cybersecurity response;
- FDA could strengthen interactions and involvement across HHS entities and with the HHS Cybersecurity Incident Response Team; and

[34] NIST Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* (September 2006).

[35] FDA, *Emergency Operations Plan*, Version 2.0 (March 2014).

- FDA needed to document formal SOPs for vulnerability management and cyber-incident response.

This weakness existed because FDA had not designed an exercise for the Cybersecurity Workgroup that involved responding to cybersecurity events affecting medical devices. Without testing scenarios specific to medical device cybersecurity, FDA was not able to take advantage of opportunities to identify previously unforeseen weaknesses or test its medical device cyber-response capabilities. After we concluded our fieldwork, but before we issued our report, FDA conducted a tabletop exercise[36] in July 2017 and provided sufficient evidence of a test scenario involving a cyberthreat to medical devices that could result in patient harm. Accordingly, we have not included a specific recommendation for this finding.

FDA HAD NOT ESTABLISHED WRITTEN STANDARD OPERATING PROCEDURES THAT ADDRESS RECALLS OF MEDICAL DEVICES VULNERABLE TO CYBERTHREATS IN 2 OF 19 DISTRICT OFFICES

Two of nineteen FDA district offices had not established written SOPs that addressed recalls of medical devices that are vulnerable to cyber vulnerabilities, exploitations, or threats. This occurred because FDA management did not have appropriate controls to ensure SOPs were in place. FDA's district office staff handle recalls in accordance with their respective district offices' SOPs. Effective documentation, such as SOPs, assists in establishing and communicating to personnel their roles and responsibilities.

As a result, in the two districts without these SOPs, FDA had an increased risk of untimely and ineffective processing of manufacturers' recalls of medical devices vulnerable to cybersecurity vulnerabilities, exploitations, and threats.

RECOMMENDATIONS

We recommend that FDA implement the specific recommendations below to enhance its ability to manage and respond to postmarket medical device compromises resulting from cybersecurity vulnerabilities, exploitations, and threats. We recommend that FDA:

- continually assess the cybersecurity risks to medical devices and update, as appropriate, its plans and strategies;

[36] Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision-making. A tabletop exercise does not involve deploying equipment or other resources (National Institute of Standards and Technology (NIST) 800-84).

- establish written procedures and practices for securely sharing sensitive information about cybersecurity events with key stakeholders who have a "need to know";

- enter into a formal agreement with Federal agency partners, namely the DHS 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

- ensure the establishment and maintenance of procedures for handling recalls of medical devices vulnerable to cybersecurity vulnerabilities, exploitations, and threats.

FDA COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, FDA agreed that the implementation of our recommendations would serve to further strengthen its operation of postmarket device cybersecurity procedures. FDA noted that it had already implemented many of the suggestions made during the audit and would continue working to implement the recommendations contained in the report.

FDA also provided written technical comments that we addressed, as appropriate. FDA's nontechnical comments are included as Appendix D.

We appreciate the efforts FDA has taken and plans to take in response to our recommendations. With respect to FDA's disagreement with some of our conclusions and findings, we maintain that they are valid for the reasons explained below.

ASSESSMENT OF MEDICAL DEVICE CYBERSECURITY

FDA Comments

FDA agreed that "[m]emorializing our engagement with the NCCIC[37] in a formal agreement will be a significant milestone in the evolution of FDA's cybersecurity framework." However, FDA disagreed with our characterization that lack of a formal agreement impedes "efficient" flow of information about cybersecurity incidents that could affect medical devices. FDA disagreed with our assertion that it "had not assessed medical device cybersecurity at an enterprise or component level."

[37] NCCIC is the DHS National Cybersecurity and Communications Integration Center, which now includes NCCIC-ICS and integrates the ICS-CERT function.

Office of Inspector General Response

Formally establishing roles, defining responsibilities, and clarifying cooperative procedures should help to ensure an effective response through a more efficient use of collective resources and the elimination of duplicative activities. Our finding and recommendation for FDA to continually assess the risk and determine which of its plans and procedures to update are supported, in part, by an email FDA sent to us stating, "2017 was the first year that FDA conducted an enterprise risk assessment [and that] CDRH was included as were all the OpDivs of FDA." After we concluded fieldwork but before we issued our draft report, FDA provided documentation supporting its first assessment of enterprise risk, which included cybersecurity risk to medical devices. Our recommendation places the responsibility on FDA management to continually assess risk and adjust its priorities and resources accordingly.

OVERSIGHT OF POSTMARKET CYBERSECURITY

FDA Comments

FDA expressed concern that "OIG fails to contextualize its observations within the extensive, well-established postmarket policies and procedures," and that our draft report provided "an incomplete and inaccurate picture of FDA's oversight of medical device cybersecurity in the postmarket phase." FDA also disagreed with our conclusion that "its preexisting policies and procedures were insufficient."

Office of Inspector General Response

The objective of our audit was to determine the effectiveness of FDA's plans and processes for timely communicating and addressing cybersecurity medical device compromises, not to report generally on FDA's postmarket policies and procedures. Further, we acknowledge that even though our fieldwork was conducted between fall 2016 and spring 2017, our report reflects actions taken by FDA subsequent to the completion of our fieldwork but before issuance of our draft report. Accordingly, our draft report takes into account FDA's actions to reduce risk and leverage existing procedures to handle cybersecurity events, including the following: (i) a *new* SOP for receiving, tracking, and fielding cybersecurity signals; (ii) a *new* charter for the Cybersecurity Workgroup; and (iii) an *updated* Triaging SOP to revise the definition of "emergency" to include certain compromises resulting from an exploitation of a cybersecurity vulnerability.

INCIDENT RESPONSE EXERCISES

FDA Comments

FDA asserted that its September 2013, March 2016, and November 2016 exercises had adequately tested its ability to respond to emergencies resulting from cybersecurity events in medical devices.

Office of Inspector General Response

We stand by our statements in our report, which are based on our analysis of the actual test results, lessons learned, and other documentation FDA provided during our audit. For its September 2013 and November 2016 exercises, FDA provided only narrative description but no additional support, such as actual test results or lessons learned. In contrast, for its July 2015 and March 2016 exercises, FDA provided additional support showing that these exercises did not involve cybersecurity events affecting medical devices. However, after our fieldwork concluded, FDA provided documentation supporting that it had tested a scenario in July 2017 involving a cyberthreat to medical devices that could result in patient harm. Accordingly, we did not include a recommendation to address this finding.

FDA OFFICE TRANSITION

FDA Comments

FDA noted that its Office of Regulatory Affairs, which conducts inspections at FDA, has transitioned away from geographically based district offices to commodity-based program division offices and therefore moved away from developing separate local office-based SOPs.

Office of Inspector General Response

We removed the term “district offices” from our recommendation.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We limited our review to FDA's policies, processes, and procedures regarding its:

- implementation of its responsibilities through regulation or other means of the Federal Food, Drug, and Cosmetic Act (Title 21 U.S.C. §§ 393 and 360i (October 4, 2016)) as it applies to medical device compromises;

- oversight of medical devices, including but not limited to medical device (a) risk assessment; (b) postmarket requirements and regulations; and (c) event triage, tracking, and management; and

- response plans for the cybersecurity risk to medical devices.

We focused our review on FDA and CDRH. We did not evaluate FDA's internal controls as a whole. We performed our fieldwork at FDA's main campus in Silver Spring, Maryland, from September 2016 to February 2017.

METHODOLOGY

To accomplish our objective, we:

- interviewed FDA's management and personnel;

- assessed FDA's policies, procedures, work instructions, manuals, guides, and practices for event risk assessment, response, handling, monitoring, and reporting;

- reviewed public information available on FDA's website;

- assessed certain FDA processes for a medical device compromise (e.g., adverse event reporting; allegations of regulatory misconduct; recalls, corrections, and removals; signal management;[38] and cybersecurity in medical devices); and

- discussed the results of our audit with FDA officials.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions

[38] The identification, evaluation, tracking, and addressing of a new potentially causal association or a new aspect of a known association between a medical device and an adverse event or set of adverse events.

based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B: FEDERAL REQUIREMENTS AND GUIDANCE

FEDERAL REQUIREMENTS

Office of Management and Budget Circular No. A-123

OMB Circular No. A-123 defines agency management's responsibilities for establishing and maintaining internal controls to achieve its strategic objectives and effective and efficient operations.

OMB Circular No. A-123 requires agencies to implement an enterprise risk management capability and to integrate risk management and internal control functions into existing business activities.

Federal leaders and managers must establish and maintain internal controls to achieve specific internal control objectives related to operations; implement management practices that identify, assess, and respond to risks; and manage both expected and unexpected or anticipated events. In addition, risk management practices must be forward-looking and designed to help decision-making, alleviate threats, and identify previously unknown opportunities to improve the efficiency and effectiveness of government operations.

Additionally, OMB Circular No. A-123 establishes an assessment process based on the Government Accountability Office's Green Book that management must implement to properly assess and improve internal controls over operations.

Government Accountability Office Standards for Internal Control in the Federal Government

The Green Book sets the standards for an effective internal control system for Federal agencies. The Green Book provides Federal managers criteria for designing, implementing, and operating an effective internal control system and sets internal control standards for Federal entities. Internal control serves as the first line of defense in safeguarding assets. Internal control comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of an entity. An effective internal control system provides reasonable assurance that management will achieve the desired results for an entity's operations.

The Green Book defines 17 principles necessary to establish an effective internal control system. The following are included among the Green Book's principles: . . .

> 3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives . . . .
>
> 6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.

> 7. Management should identify, analyze, and respond to risks related to achieving the defined objectives . . . .
>
> 9. Management should identify, analyze, and respond to significant changes that could impact the internal control system . . . .
>
> 11. Management should design the entity's information system and [implement] related control activities [through policies] to achieve objectives and respond to risks . . . .
>
> 13. Management should use quality information [and internally and externally communicate that information] to achieve the entity's objectives . . . .
>
> 16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.
>
> 17. Management should remediate identified internal control deficiencies on a timely basis.

In addition, the Green Book includes minimum documentation requirements. The following are included among the requirements:

> If management determines that a principle is not relevant, management supports that determination with documentation that includes the rationale of how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively . . . .
>
> Management develops and maintains documentation of its internal control system . . . .
>
> Management documents in policies the internal control responsibilities of the organization . . . .
>
> Management evaluates and documents the results of ongoing monitoring and separate evaluations to identify internal control issues . . . .
>
> Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies on a timely basis.

Department of Health and Human Services Working Group Standard Operating Procedures

According to HHS's Working Group SOP, "Working groups[39] are . . . forums for discussion and building consensus around important topic areas. In moving towards using working groups as a means to collaborate and share information across the Department . . .," it is critical that HHS Operating and Staff Divisions formalize all working groups that have relevance to cybersecurity and that their operations are standardized. The HHS Working Group SOP requires all HHS working groups to develop and maintain a charter.

FEDERAL GUIDANCE

National Institute of Standards and Technology

NIST Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, provides guidance on designing, developing, conducting, and evaluating test, training, and exercise events to aid personnel in preparing for adverse situations involving IT. Organizations need to maintain IT capabilities, such as incident response capabilities, to sustain the organization's ability to prepare for, respond to, manage, and recover from adverse situations involving IT.

[39] According to the HHS Working Group SOP, a working group is an interdisciplinary collaboration of key stakeholders, individuals, and subject matter experts working to address a systemic or Department-wide problem, requirement, or emerging topic of interest.

APPENDIX C: "FDA Fact Sheet, The FDA's Role in Medical Device Cybersecurity, Dispelling Myths and Understanding Facts"[40]

Myths	Facts
The FDA is the only Federal Government agency responsible for the cybersecurity of medical devices.	The FDA works closely with several Federal Government agencies including the U.S. Department of Homeland Security (DHS), members of the private sector, medical device manufacturers, health care delivery organizations, security researchers, and end users to increase the security of the U.S. critical cyber infrastructure.
Medical device manufacturers can't update medical devices for cybersecurity.	Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity.
Health care Delivery Organizations (HDOs) can't update and patch medical devices for cybersecurity.	The FDA recognizes that HDOs are responsible for implementing devices on their networks and may need to patch or change devices and/or supporting infrastructure to reduce security risks. Recognizing that changes require risk assessment, the FDA recommends working closely with medical device manufacturers to communicate changes that are necessary.
The FDA is responsible for the validation of software changes made to address cybersecurity vulnerabilities.	The medical device manufacturer is responsible for the validation of all software design changes, including computer software changes to address cybersecurity vulnerabilities.
The FDA tests medical devices for cybersecurity.	The FDA does not conduct premarket testing for medical products. Testing is the responsibility of the medical product manufacturer.

[40] Accessed at https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf on April 6, 2018.

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration
Silver Spring MD 20993

DATE: August 13, 2018

TO: Inspector General

FROM: Deputy Associate Commissioner for Public Health Strategy and Analysis

SUBJECT: FDA's General Comments to OIG Draft Report, "The Food and Drug Administration's Policies and Procedures Did Not Adequately Address Cybersecurity Risk to Medical Devices" (A-18-16-30530)

FDA is providing the attached general comments to the OIG Draft Report, "The Food and Drug Administration's Policies and Procedures Did Not Adequately Address Cybersecurity Risk to Medical Devices" (A-18-16-30530).

We appreciate the opportunity to review and comment on this draft report before it is published.

Lisa Rovin
Deputy Associate Commissioner for Public Health
Strategy and Analysis

Attachment

The Food and Drug Administration's General Comments to OIG Draft Report, "The Food and Drug Administration's Policies and Procedures Did Not Adequately Address Cybersecurity Risk to Medical Devices" (A-18-16-30530)

The Food and Drug Administration (FDA or the Agency) appreciates the opportunity to comment on this draft report.

Cybersecurity is critical to the safety and effectiveness of networked medical devices, and FDA's Center for Devices and Radiological Health (CDRH) leads the Agency's regulatory oversight of cybersecurity. Over the past five years, the FDA, through CDRH's leadership, has built a comprehensive regulatory framework for addressing potential cybersecurity threats both before and after a networked medical device comes to market. FDA is pleased to provide more information about that regulatory framework and respond to the specific observations and recommendations in OIG's draft report.

In FDA's view, the OIG draft report provides an incomplete and inaccurate picture of FDA's oversight of medical device cybersecurity in the postmarket phase. Specifically, FDA notes that fieldwork for the audit was primarily conducted during Fall 2016-Spring 2017, during which time FDA finalized its guidance on postmarket medical device cybersecurity; since then, FDA has continued to build out its cybersecurity framework, as described in more detail below. In addition, in FDA's view, OIG overstates the significance of its observations (*e.g.*, that FDA had not created a group email account or electronic mailbox for the Cybersecurity Workgroup) in relation to FDA's device cybersecurity framework and the underlying standards against which FDA's performance was evaluated. Moreover, as OIG notes, FDA has already implemented many of the suggestions that OIG made during the course of the audit. Accordingly, although FDA agrees that implementation of OIG's recommendations will serve to further strengthen operation of postmarket device cybersecurity procedures, FDA disagrees with the conclusion that its preexisting policies and procedures were insufficient or that the absence of the documentation recommended by OIG "put at risk" the effectiveness of certain regulatory oversight functions. Nevertheless, FDA has worked diligently throughout OIG's review to respond to the team's observations, and FDA will continue working to execute the recommendations contained in the report.

FDA's Role in Advancing Medical Device Cybersecurity

For context, FDA's current approach to advancing medical device cybersecurity, through implementation of a regulatory framework as well as active stakeholder engagement, is described below.

FDA is responsible for ensuring that patients and healthcare providers have access to safe and effective medical devices. This applies throughout the "total product life cycle" of a device—starting with FDA's review of a device before it comes to market, and continuing through surveillance and regulatory oversight in the postmarket setting. In recent years, an important aspect of FDA's regulatory framework has included identification, protection, detection, and response to potential cybersecurity vulnerabilities in networked medical devices. For this reason, FDA does not compartmentalize its premarket and postmarket activities, nor assesses them in isolation. Instead, FDA has taken a holistic, systematic approach to building its cybersecurity program, as well as to creating an environment of shared responsibility with industry and other stakeholders. The infrastructure-building has encompassed both policy and process, including the following key steps:

- Establishing a team within CDRH's Office of the Center Director that is specifically dedicated to medical device cybersecurity policy development, preparedness, coordination within and outside CDRH, and incident response. Led by the Associate Director for Science & Strategic

The Food and Drug Administration's General Comments to OIG Draft Report, "The Food and Drug Administration's Policies and Procedures Did Not Adequately Address Cybersecurity Risk to Medical Devices" (A-18-16-30530)

Partnerships, the team is responsible for developing the cybersecurity program within CDRH and leading the Agency's response to potential threats and incidents, such as the impact of WannaCry on vulnerable medical devices in the United States. It coordinates operation of the CDRH Cybersecurity Workgroup, a cross-functional group of representatives from offices throughout the Center that fulfills important internal advisory, analysis and communication functions.

- Issuing two guidance documents that establish a framework to address premarket and postmarket regulatory considerations.
    - In October 2014, FDA published *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, which identified issues that manufacturers should consider in the design and development of their medical devices.[1]
    - In December 2016, FDA issued *Postmarket Management of Cybersecurity in Medical Devices*, setting forth an innovative, risk-based framework for the Agency's postmarket oversight.[2]
    - Each guidance was implemented by promoting external awareness through FDA-convened stakeholder webinars and conference presentations, as well as by conducting internal staff training across CDRH reviewer and analyst divisions.

- Engaging formally and informally with diverse stakeholders—within HHS, with other government agencies, with private industry, and others—to gain insight on device lifecycle challenges, policy needs, and to leverage potential regulatory science tools and approaches to address current gaps.
    - For instance, CDRH has convened three public workshops (in 2014, 2016, and 2017) to address device cybersecurity topics.
    - Its team members regularly attend industry and cybersecurity conferences to exchange insights with healthcare delivery organizations (HDOs), security researchers, industry experts, academics, clinicians, patients and others across both the private sector and government.
    - CDRH contributed expertise as a steering committee member to the Health Care Industry Cybersecurity (HCIC) Task Force during development of its Task Force Report, issued to Congress in June 2017.
    - CDRH currently serves as a co-chair of the Healthcare and Public Health Sector Government Coordinating Council, a body that facilitates interagency and cross-jurisdictional cooperation for protecting critical infrastructure.
    - CDRH currently co-chairs the Medical Technology and Health IT Task Group of the Healthcare Sector Coordinating Council. This task group is currently drafting the "Joint

[1] *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, Guidance for Industry and Food and Drug Administration Staff (Oct. 2, 2014), available at: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.
[2] *Postmarket Management of Cybersecurity in Medical Devices*, Guidance for Industry and Food and Drug Administration Staff (Dec. 28, 2016), available at: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

The Food and Drug Administration's General Comments to OIG Draft Report, "The Food and Drug Administration's Policies and Procedures Did Not Adequately Address Cybersecurity Risk to Medical Devices" (A-18-16-30530)

Security Plan" (JSP), a shared vision with best practices for implementing the medical device security and resilience recommendations published in the HCIC Task Force Report.

- CDRH actively encourages collaboration among government entities, medical device manufacturers, health care delivery organizations (hospitals and others), cybersecurity researchers, clinicians and patients to foster a shared responsibility for the cybersecurity of medical devices.

- Conducting or participating in mock cybersecurity attack exercises. CDRH understands the importance of cybersecurity preparedness and of exercising response plans to enable the protection of patient safety, the healthcare and public health critical infrastructure, and national security. Since 2013, CDRH has actively led and/or contributed to and participated in six functional or tabletop exercises to evaluate its own response capabilities, as well as those of affected industry and healthcare stakeholders. In each case, CDRH has gained important insights, which it has translated into subsequent programmatic enhancements designed to facilitate an agile, effective response to any actual incident.

- Developing and formalizing collaborative working relationships:
  - CDRH coordinates with the National Cybersecurity and Communications Integration Center (NCCIC), the Department of Homeland Security's cyber situational awareness, incident response, and management center. Through regular communications with NCCIC staff, CDRH contributes clinical and subject matter expertise to the evaluation of potential medical device cybersecurity vulnerabilities and helps facilitate resolutions to vulnerability coordination issues.
  - CDRH supports the formation of medical device Information Sharing and Analysis Organizations (ISAOs) and partnering with the National Health Information Sharing and Analysis Center (NH-ISAC) that together, serve to broadly reduce risk across the HPH sector by sharing information on medical device vulnerabilities and effective solutions.
  - CDRH has begun to establish collaborations with entities that can provide a clinical sandbox/test-bed to conduct impact analyses of medical device vulnerabilities in a patient simulation setting as well as to evaluate fixes.

Through these activities and others, FDA has become well-respected for thought leadership on cybersecurity issues and has earned a reputation as a nimble regulator. Like the evolving nature of the devices regulated—and cybersecurity threats faced—FDA's regulatory approach is not static. FDA continues to refine and expand the regulatory framework that it has put in place. For instance, as outlined in the *Medical Device Safety Action Plan* that CDRH published this year, the Agency has identified several important policy efforts that will continue to advance its device cybersecurity program.[3] Specifically, FDA intends to:

[3] FDA, *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health*, available at: https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf.

The Food and Drug Administration's General Comments to OIG Draft Report, "The Food and Drug Administration's Policies and Procedures Did Not Adequately Address Cybersecurity Risk to Medical Devices" (A-18-16-30530)

- Later this year, issue an updated premarket guidance on medical device cybersecurity to better protect against moderate risks (such as ransomware campaigns that could disrupt clinical operations and delay patient care) and major risks (such as exploiting a vulnerability that enables a remote cybersecurity attack) based on the knowledge we have acquired since we first issued the guidance in 2014;
- Consider potential new premarket authorities that would require firms, on the front end, to take additional steps to secure their devices—such as building capability to update and patch device security into a product's design, and developing a "Software Bill of Materials" that will enable device customers and users to better manage their networked asset;
- Consider potential new postmarket authorities that would require firms to adopt policies and procedures for coordinated disclosure of vulnerabilities as they are identified; and
- Explore development of a public-private partnership, a "CyberMed Safety (Expert) Analysis Board," that would complement existing device vulnerability coordination and response mechanisms through, among other things, assessing vulnerabilities, evaluating patient safety risks, adjudicating disputes, assessing proposed mitigations, serving in a consultative role to organizations navigating the coordinated disclosure process, and serving as a "go-team" that could be deployed in the field to investigate a suspected or confirmed device compromise at a manufacturer's or FDA's request.

FDA looks forward to further advancing its medical device cybersecurity program in ways that will continue to protect patients and promote public health.

FDA's Response to the OIG's Findings and Recommendations

All stakeholders, including FDA, must strive to keep pace with emerging device cybersecurity vulnerabilities and threats. Continuous improvement is essential for an effective cybersecurity program, and FDA takes seriously OIG's observations and recommendations for improvement.

FDA made the proactive decision to take steps to address cybersecurity vulnerabilities and incidents before all the components of its program had been fully implemented because of the emerging public health threat of cybersecurity attacks. OIG began its audit even as FDA was still implementing the program, and OIG's background summary as well as its findings provide an incomplete snapshot of FDA's work. Nevertheless, FDA has worked proactively to address the OIG's preliminary observations and recommendations, many of which were steps that FDA had been in the process of implementing or planned to implement at the time of the audit. As OIG notes, FDA has now implemented many of the suggestions that OIG made during the course of the audit. Importantly, OIG notes that it did not find evidence that FDA had mismanaged or responded untimely to a reported medical device cybersecurity event.

Fundamentally, FDA disagrees with OIG's conclusion that FDA's policies and procedures did not "adequately" address cybersecurity risk to medical devices. To support this conclusion, the draft report (1) enumerates a list of procedures, resources, or other documentation that OIG asserts should have been developed to address handling postmarket cybersecurity events, (2) describes additional work that should have been done to test emergency scenarios (which FDA subsequently completed); and (3) notes that 2 of FDA's 19 district offices do not maintain written standard operating procedures that address recalls due to

The Food and Drug Administration's General Comments to OIG Draft Report, "The Food and Drug Administration's Policies and Procedures Did Not Adequately Address Cybersecurity Risk to Medical Devices" (A-18-16-30530)

cybersecurity threats. FDA agrees that the documentation and formalization of processes recommended by OIG are appropriate and useful, but does not agree that they are necessary to meet an undefined threshold of "adequacy" or that their absence "put at risk" the effectiveness of certain regulatory oversight functions.

With respect to the first observation, FDA is particularly concerned that OIG fails to contextualize its observations within the extensive, well-established postmarket policies and procedures that FDA relies upon for any postmarket safety event, including those related to cybersecurity. These policies and processes—including for receipt of medical device reports (reports of certain adverse events and device malfunctions); response to manufacturer reports of corrections and removals; inspection of device establishments for compliance with quality system and other applicable requirements; and response to complaints or allegations made by members of the public—are the backbone of FDA's postmarket device surveillance program. During the course of the audit, FDA expended considerable time and resources in providing these (and other) materials for OIG's review. While the additional documentation recommended by OIG will enhance the FDA's operation of its program, it simply does not follow that their absence rendered FDA's existing policies and procedures "inadequate."

In addition, CDRH has built a strong, collaborative working relationship with the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), now known as the NCCIC. Memorializing our engagement with the NCCIC in a formal agreement will be a significant milestone in the evolution of FDA's cybersecurity framework; however, FDA disagrees with OIG's characterization that lack of a formal agreement impedes "efficient" flow of information about cybersecurity incidents that could affect medical devices.

FDA is also concerned with OIG's assertion that the Agency had not assessed medical device cybersecurity at an enterprise or component level. As outlined above, FDA has built a multi-faceted regulatory program specifically dedicated to mitigating the risk of cybersecurity threats to medical devices, from their inception to obsolescence. The existence of this program reflects the Agency's assessment of the significance of device cybersecurity risk. Moreover, CDRH had documented its assessment of medical device cybersecurity in the Agency's enterprise risk assessment, independent of the ongoing OIG audit.

FDA also disagrees with the assertion that it had not adequately tested its ability to respond to emergencies resulting from cybersecurity events in medical devices. FDA fully appreciates the importance of training and exercises to help ensure that personnel are able to respond to and manage emergency situations. Since 2013, CDRH has actively led and/or contributed and participated in cross-sector and sector-specific cybersecurity exercises, and it continues proactively to do so. Specifically:

- In September 2013, CDRH collaborated with the NCCIC to help plan, and then participated in, a 3-day functional exercise that deliberately included a medical device exploit scenario that resulted in patient harm, designed by CDRH.
- In March 2016, CDRH again collaborated with Department of Homeland Security to plan and participate in a capstone national level exercise, including providing a medical device scenario for potential use.

The Food and Drug Administration's General Comments to OIG Draft Report, "The Food and Drug Administration's Policies and Procedures Did Not Adequately Address Cybersecurity Risk to Medical Devices" (A-18-16-30530)

- In November 2016, CDRH participated in the AdvaMed Cybersecurity Summit, in which a medical device sector-specific tabletop exercise evaluated industry response to a targeted ransomware attack that impacted a medical device's functionality and potential for patient harm.

These activities occurred prior to the close of OIG fieldwork for this draft report. Subsequently, CDRH has engaged in several additional tabletop exercises, including at the NH-ISAC/MDISS and Smiths Medical Summit (June 2017); through an exercise led by HHS's Assistant Secretary for Preparedness and Response (July 2017); and through an industry exercise that CDRH coordinated with the MITRE Corporation to advance development of policies and procedures related to disclosure of medical device cybersecurity vulnerabilities (July 2017). As a result of these exercises, CDRH identified the need for response "playbooks" to outline best practices for multi-stakeholder communication and coordination in response to device cybersecurity incidents. FDA, with MITRE, is currently developing drafts of two playbooks—one to serve as a guide for stakeholders (*e.g.*, hospital systems and other health care delivery organizations), and one as an internal resource for FDA—which are expected to publish by the end of 2018.

FDA also notes that since the time that OIG conducted this audit, FDA's Office of Regulatory Affairs (ORA), the office that conducts inspections at FDA, has transitioned away from geographically based district offices to commodity-based program division offices. The transition has been a major effort aimed at achieving consistency and efficiencies across commodity programs, including moving away from developing separate local office-based SOPs. Because of this transition, the use of the term "district office" throughout the report no longer accurately reflects ORA's current organization structure. The Regulatory Procedures Manual (RPM) is the current national recall procedure that should be followed by the field and FDA headquarter offices, including CDRH. The RPM does not include commodity-specific recall procedures; rather, it includes procedures that apply to all commodities and would encompass recall procedures for various types of situations. Thus, it would cover handling recalls of medical devices vulnerable to cybersecurity vulnerabilities.

Additionally, FDA leadership approved and implemented an enterprise-wide recall audit plan in October 2016, that utilizes ORA's quality management system. We provided a copy of this audit plan to the OIG during the study.

Conclusion

Potential threats to the cybersecurity of medical devices pose a serious, emerging risk. FDA is proud of the work it has done not only to build a framework that specifically addresses this risk and with sufficient latitude to continuously evolve, but also to foster a far broader, collaborative approach amongst government, industry, health care providers, security researchers, clinicians, patients and others. FDA recognizes that opportunities to refine and enhance its program remain.

The draft report includes four specific recommendations to enhance FDA's ability to manage and respond to cybersecurity vulnerabilities, exploitations, and threats:

1. Continually assess the cybersecurity risks to medical devices and update, as appropriate, its plans and strategies;

The Food and Drug Administration's General Comments to OIG Draft Report, "The Food and Drug Administration's Policies and Procedures Did Not Adequately Address Cybersecurity Risk to Medical Devices" (A-18-16-30530)

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 DHS 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 all district offices establish and maintain a written SOP for handling recalls of medical devices vulnerable to cybersecurity vulnerabilities, exploitations, and threats.

FDA has already taken steps to implement these recommendations, and plans to update OIG as these items are completed. FDA appreciates the opportunity to provides these comments to OIG.