For Immediate Release

September 27, 2012

Contact: Kristin Kopshever (202) 225-6375

Kristin.Kopshever@mail.house.gov

Reps. Edwards, Eshoo, Markey: Hacking Threats to Implantable Medical Devices Call For Improved FDA Oversight

(Washington, DC) – Reacting to the findings of a new Government Accountability Office (GAO) report they requested last year, three senior House Democrats today are calling on the Food and Drug Administration (FDA) to improve its oversight of implantable wireless medical devices. In recent demonstrations, computer security experts revealed that some implantable medical devices can be remotely controlled by a hacker, posing potentially serious health risks to patients.

The GAO report, ***"MEDICAL DEVICES: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices,"*** found that both the FDA and medical device manufacturers have been slow to respond to this emerging threat. "FDA has not considered information security risks resulting from intentional threats," the GAO concluded. More specifically, the agency failed to consider "intentional threats" in the pre-market approval and evaluation of two devices that were successfully hacked, an implantable cardiac defibrillator and insulin pump. The GAO also found that the FDA has not utilized resources available from other government agencies, particularly the National Institute of Standards and Technology (NIST), which maintains a federal computer security vulnerability database and provides guidance and standards related to computer security.

The three lawmakers who requested the review were: **Ms. Donna F. Edwards**, Ranking Member, Subcommittee on Technology and Innovation, Committee on Science, Space and Technology, **Ms. Anna G. Eshoo**, Ranking Member, Subcommittee on Communications and Technology, Committee on Energy and Commerce and Co-chair of the House Medical Technology Caucus and **Mr. Edward J. Markey**, former Chairman of the telecommunications subcommittee and current senior member of the Energy and Commerce Committee.

"It is unacceptable that the Food and Drug Administration is ignoring the resources of other government agencies in evaluating life-saving medical devices," said **Rep. Edwards**. "In the future, I expect the agency to utilize the computer security expertise offered by NIST and other federal agencies to assess the security risks posed by these devices. The FDA must address potential threats and close security gaps in order to have the full confidence of Congress and the American people."

"Wireless medical devices are susceptible to increasingly advanced hacking techniques that could threaten patient health," said **Rep. Markey**. "Patients need to be informed about whether the medical devices implanted in their bodies contain security vulnerabilities that could harm them so they can take appropriate precautions whenever possible. This report underscores the need to

require manufacturers to acknowledge these threats and for FDA to address the risks before the devices are sold to the public."

"Even the human body is vulnerable to attack from computer hackers," said **Rep. Eshoo**. "Implantable medical devices have resulted in tremendous medical benefits for the patients who use them, but the demonstrated security risks require a renewed emphasis by the FDA and manufacturers to identify, evaluate and plug the potentially rare but serious security holes that exist in these devices."

GAO Recommendations

To address security issues, the GAO recommends in the report that the Secretary of the Department of Health and Human Services direct the Commissioner of the FDA to develop and implement a more comprehensive plan to assist FDA in enhancing its review and surveillance of medical devices that more fully incorporates information security into these devices. The GAO listed four actions by the FDA that should be included in this plan:

1) The FDA should increase its focus on manufacturers' identification of potential unintentional and intentional computer security threats and vulnerabilities and strategies to mitigate these risks during its pre-market approval review process;

2) Utilize available resources, including those from other entities, such as other federal agencies;

3) Leverage its post-market efforts to identify and investigate information security problems; and

4) Establish a specific schedule for completing this review and implementing these changes.

The GAO report, ***MEDICAL DEVICES: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices,"*** GAO-12-816, September 2012, will be available here: http://www.gao.gov/products/GAO-12-816

Additionally, a one page backgrounder on the GAO's findings is attached to this release.

Press Contacts:

Ms. Donna F. Edwards, contact Dan Weber, Communications Director
(202)-225-8699; Dan.Weber@mail.house.gov

Ms. Anna G. Eshoo, contact Charles Stewart, Communications Director
(202) 225-8104; Charles.Stewart@mail.house.gov

Mr. Edward J. Markey, contact Giselle Barry, Communications Director
202-225-2836; Giselle.barry@mail.house.gov

September 27, 2012 (Backgrounder – Prepared by Committee Staff)

Medical Devices: FDA Should Expand its Consideration of Information Security for Certain Types of Devices *(GAO 12-816)*

Rep. Donna F. Edwards, Ranking Member, Subcommittee on Technology and Innovation, Committee on Science, Space and Technology, **Rep. Edward J. Markey**, Ranking Member of the Committee on Natural Resources, and **Rep. Anna G. Eshoo**, Ranking Member of the Subcommittee on Communications and Technology and Co-chair of the House Medical Technology Caucus, requested a GAO report on the information security of implantable wireless medical devices. They requested the report after computer security experts demonstrated that certain devices could be intentionally breached by hackers.

BACKGROUND

Today, more than 25 million Americans rely on implantable medical devices and this number is expected to grow rapidly in the next few years. These devices include deep brain stimulators to help alleviate epileptic seizures, cardiac defibrillators, which use electricity to control irregular heartbeats, and insulin pumps that dispense insulin to diabetics. These devices have saved lives and improved the health of millions. However, since 2008 there have been at least four separate laboratory demonstrations showing wireless medical devices can be intentionally manipulated without proper authorization.

The Food and Drug Administration (FDA) is responsible for approving and ensuring the safety and effectiveness of all medical devices. According to the GAO, the FDA did not consider intentional information security risks as a realistic possibility until recently. Additionally, although the agency intends to reassess its approach to reviewing software used in medical devices, it does not plan to specifically address information security as part of this effort.

Manufacturers of these devices have also been exceedingly slow to publicly acknowledge these potential computer security risks. Manufacturers are required to include information about known defects in their devices in published material. However, the GAO found that the manufacturers of the two devices that were intentionally manipulated in the laboratory, a cardiac defibrillator and insulin pump, both failed to include information about known security vulnerabilities in their corporate annual reports and other publications.

RECOMMENDATIONS

The GAO recommends that the FDA develop and implement a more comprehensive plan to enhance its review and oversight of medical devices that more fully addresses the information security risks of these devices. The GAO listed four minimum actions the FDA should include in this plan:

1. Increase its focus on manufacturers' identification of potential unintentional and intentional computer security threats and vulnerabilities and strategies to mitigate these risks during its pre-market approval review process;

2. Utilize available resources, including those from other entities, such as other federal agencies, particularly the National Institute of Standards and Technology (NIST);

3. Leverage its post-market efforts to identify information security problems; and

4. Establish a specific schedule for completing this review and implementing these changes.