INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

March 30, 2012

The Honorable Jeffrey Zients
Acting Director, US Office of Management and Budget
Washington, DC 20502

Dear Mr. Zients,

I am writing to you as the Chair of the Information Security and Privacy Advisory Board (ISPAB or Board). The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-35) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002. One of the statutory objectives of the Board is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

At the Board meeting of February 1-3, 2012, the Board discussed the issue of maintaining security in medical devices that are increasingly operated by software connected to the public Internet, possibly through wireless connections. The Board heard experts discuss how lack of cybersecurity preparedness for millions of software-controlled medical devices puts patients at significant risk of harm. Specifically, software-controlled medical devices are increasingly available through and exposed to cybersecurity risks on the Internet; examples range from desktop computers controlling radiological imaging to custom embedded software found in pacemakers. With increasing connectivity comes greater functionality and manageability, but also increased risks of both unintentional interference and malicious tampering via these communication channels.

Further complicating this picture, the economics of medical device cybersecurity involves a complex system of payments between multiple stakeholders -- including manufacturers, providers, and patients. At the same time, no one agency has primary responsibility from Congress to ensure the cybersecurity of medical devices deployed across this spectrum;

Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-2938 *** Fax: 301/975-4007

agencies involved include Centers for Medicare and Medicaid Services (CMS) and Food and Drug Administration (FDA) in Department of Health and Human Services (HHS), as well as the Department of Defense (DOD), Department of Veterans' Affairs (VA), and Department of Homeland Security (DHS), among others. Given the complexity of the technical issues involved, the Board finds that diffusion of responsibility when it comes to cybersecurity of medical devices raises growing concern.

In addition, there is an economic disincentive for reporting of vulnerabilities and incidents – a hospital, for example, can incur liability by reporting a problem. A lack of meaningful data on medical device cybersecurity can lead to cybersecurity unpreparedness because cybersecurity problems that go unreported can increase a false impression of preparedness due to lower incident counts. This lack of reported incidents also results from a lack of effective reporting mechanisms from clinical settings to the Government about cybersecurity threats in medical devices.

The Board made the following observations from the panel discussion:

- There is a diffusion of Government responsibility for cybersecurity of medical devices, leading to lack of accountability and oversight.

- Current medical device reporting methods, primarily captured through FDA, are not designed to capture indicators of medical device cybersecurity problems.

- Medical devices used in the home raise additional cybersecurity risks, given the less trustworthy nature of the home environment.

- The Government has multiple ways to address cybersecurity for medical devices, including regulation through FDA, purchasing power through CMS, information distribution through numerous agencies, and education and awareness to home users and medical providers.

Based on the Board's discussion and findings, we offer a number of recommendations:

1. A single Federal entity (such as FDA) should be assigned responsibility for taking medical device cybersecurity into account during pre-market clearance and approval of devices, and during post-market surveillance of cybersecurity threat indicators at time of use.

2. FDA should collaborate with National Institute of Standards and Technology (NIST) scientists and engineers to research cybersecurity features that could be enabled by default on networked or wireless medical devices in Federal settings. For instance, a

medical provider should not have to download new software, such as an anti-virus product, to achieve an acceptable baseline of cybersecurity. Cybersecurity features in medical devices should be active at the time of purchase by the Government, and should be easily and transparently configurable by a provider at the time of use; this can translate into improved cybersecurity in device acquisition across a broad spectrum of buyers.

3. The Government should assign a lead entity (such as Health Resources and Services Administration (HRSA) or FDA in HHS) to establish better training and education that informs users, health care organizations, and manufacturers about the risks associated with networked and wireless medical devices. This lead organization should make information readily available to all parties upon receipt of a medical device, as well as part of the "instructions for use" for the users.

4. Because medical devices are increasingly Internet-based, United States Computer Emergency Readiness Team (US-CERT) should create defined reporting categories for medical device cybersecurity incidents. Coordination is necessary with US-CERT to establish mechanisms that incentivize Government, providers, and manufacturers to collect cybersecurity threat indicators so that the country is prepared for the inevitable growth in device incident reports.

5. Further study is needed to determine whether additional policy or legislative changes are necessary to promote medical device security.

The Board appreciates the opportunity to provide views on this emerging and important issue. We welcome further discussion at the Administration's discretion.

Sincerely,

Daniel J. Chenok
Chair, ISPAB

cc: The Honorable Kathleen Sebelius, Secretary, Department of Health and Human Services
Steven VanRoekel, Administrator of E-Government and Information Technology and CIO, OMB
Howard Schmidt, Cybersecurity Coordinator, National Security Council,
Mark Weatherford, Deputy Undersecretary for Cybersecurity, DHS
Patrick Gallagher, Director, NIST