Welcome to today's
FDA/CDRH Webinar

Thank you for your patience while we register all of today's participants.

If you have not connected to the audio portion of the webinar, please do so now:

Dial: 888-456-0356

International Callers:1-517-308-9409

Passcode:9748303

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Abiy Desta
Office of the Center Director
Center for Devices and Radiological Health

Purpose

On October 1, 2014 FDA published a guidance document with recommendations on how companies should document their approach to managing cybersecurity risk medical devices in their pre-market submissions. The purpose of this webinar is to help clarify the Agency's recommendations and answer questions related to the content of the guidance document.

Background

- FDA's guidance document represents the Food and Drug Administration's current thinking on this topic
  - should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited
  - alternative approaches my be used
- On October 1, 2014, FDA published a final guidance on recommendations to consider and information to include in FDA medical device premarket submissions for effective cybersecurity management

Introduction

- Manufacturers should incorporate specific controls into the design of their products to address cybersecurity
- Manufacturers should consider the risk to patients from a malfunction as well as the environment in which the device is used
- FDA recognizes that medical device security is a shared responsibility between stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices.

Scope

- This guidance is applicable to all premarket submissions containing software, programmable logic, and standalone software that is a medical device.

Core Functions to Consider

- **Identify and Protect**
  - Limit access to trusted users
    - Layered privileges
    - Appropriate authentication
    - Strengthen password
  - Terminate session after a period of inactivity
  - Limit access to minimize tampering
    - Physical lock
    - Limit access ports

Core Functions to Consider

- **Detect, Respond, and Recover**
  - Implement features that allow users to learn that the device has been compromised
  - Provide information on appropriate actions to take once device has been compromised
  - Implement features that preserve critical functions including:
    - Ability to reboot
    - Ability to recognize drivers
  - Provide methods for retention and recovery of device configuration

Documentation

- **Hazard analyses**
  - Evaluate both intentional and unintentional cybersecurity risk
    - Provide information on the risk analyzed
  - Controls established to mitigate risk
    - Provide information on the controls put in place
    - Provide information on the appropriateness of the controls to mitigate identified risk
  - Matrix that links cybersecurity controls to the risk being mitigated
  - Summary documentation on
    - Plan to provide validated patches / updates
    - Plan to assure device integrity
  - Devices instruction related to cybersecurity

Conclusion

- **The FDA recognizes some consensus standards, which are listed on page seven of this guidance .**
- **Manufacturers may choose alternative approaches to implementing cyber security controls**
  - Have controls in place
  - Demonstrate to the agency the appropriateness of those controls in the premarket submission.
- **Recognize the threat is continuously evolving and have a plan in place to appropriately manage the evolving threat.**

Questions?

Division of Industry and Consumer Education:
DICE@fda.hhs.gov

Slide Presentation, Transcript and Webinar Recording will be available at:

www.fda.gov/CDRHWebinar under the "Past Webinars and Stakeholder Calls-2014" tab.