

# **MEDICAL DEVICE CYBERSECURITY: Through The FDA Lens**

Suzanne B. Schwartz, MD, MBA  
FDA Center for Devices and Radiological Health  
USENIX 2018, Baltimore Maryland  
Aug 17, 2018

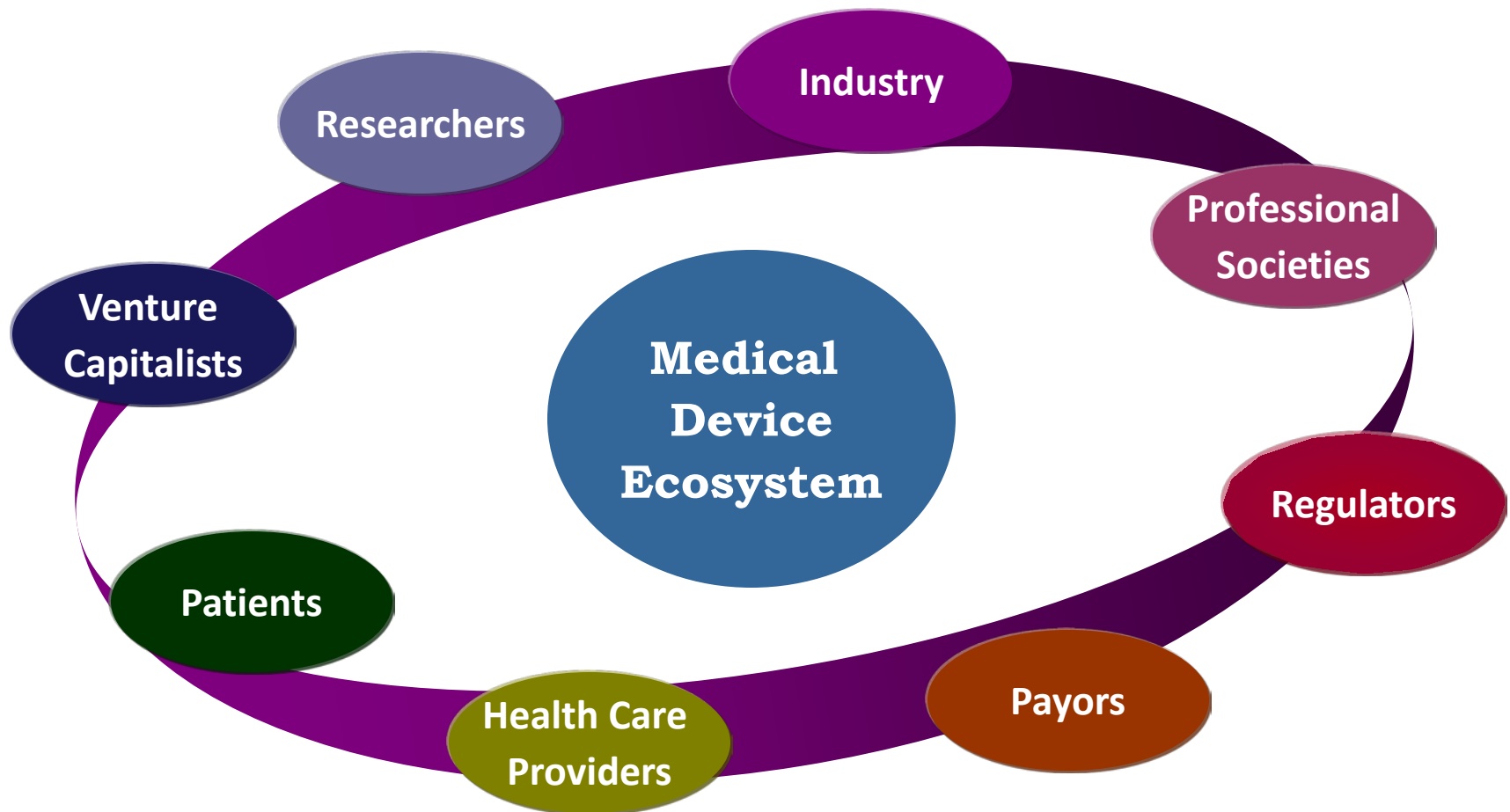
# Framing the Issue: Environment

- The healthcare and public health (HPH) critical infrastructure sector represents a significantly large attack surface for national security today
  - Intrusions and breaches occur through weaknesses in the system architecture
- Connected medical devices, like all other computer systems, incorporate software that is vulnerable to threats
- Cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations
- When medical device vulnerabilities are not addressed and remediated, they can serve as access points for entry into hospital/healthcare facility networks
  - May lead to compromise of data confidentiality, integrity, and availability
  - May lead to compromise of essential performance

## Bottom Line Up Front (BLUF)

- “*Whole of community*” approach: Collaboration is key
- Security spans across the total product lifecycle
- Impact on critical infrastructure within and across sectors
- Shifting the mindset:
  - Consider scenarios beyond “intended use”
  - Integrate threat modeling
  - Beware of using probabilistic determinations—these can yield a false sense of security
- Foster culture and create incentives that encourage proactive behavior, *especially for information sharing*
- Major strides made AND acceleration necessary

# Ecosystem Stakeholders

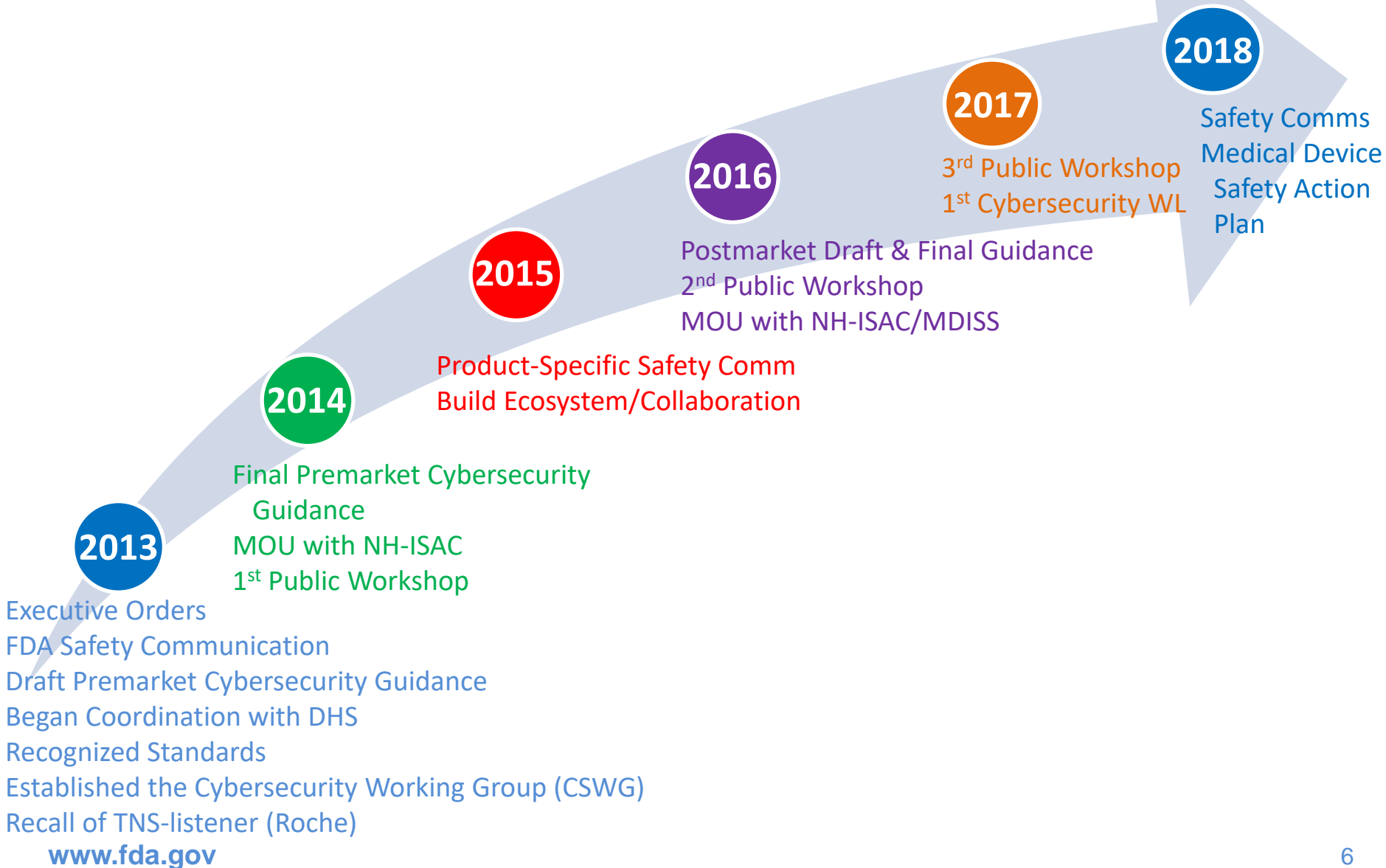


# Framework to Strengthen Cybersecurity and Critical Infrastructure

- Federal policy framework for cybersecurity and critical infrastructure resilience emphasizes a collaborative approach among government, industry and other stakeholders; establishment of Information Sharing and Analysis Organizations (ISAOs); and support for cybersecurity risk management efforts to protect critical infrastructure
  - Executive Order 13636, Improving Critical Infrastructure Cybersecurity (*“We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.”*)
  - Presidential Policy Directive 21, Critical Infrastructure Security and Resilience
  - Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing (encouraging voluntary establishment of ISAOs as a mechanism for entities to share information related to cybersecurity risks and incidents and to respond collaboratively in as close to real time as possible)
  - Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (support for cybersecurity efforts of critical infrastructure entities)
- National Institute of Standards and Technology (NIST) Voluntary Framework (v1.0 - Feb 2014, v1.1 – April 2018)



# FDA Cybersecurity History



# FDA Cybersecurity Work Products



U.S. Department of Health and Human Services  
**FDA U.S. FOOD & DRUG ADMINISTRATION**  
 Home | Food | Drugs | Medical Devices | Radiation-Emitting Products | Vaccines, Blood & Biologics | Animal & Veterinary | Cosmetics | Tobacco Products

Medical Devices  
 Home > Medical Devices > Digital Health

**Digital Health**  
 Cybersecurity

Health IT Risk-Based Framework  
 Medical Device Interoperability  
 Mobile Medical Applications  
 Wireless Medical Devices

**Cybersecurity**

Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. This vulnerability increases as medical devices are increasingly connected to the Internet, hospital networks, and to other medical devices.

All medical devices carry a certain amount of risk. The FDA allows devices to be marketed when there is a reasonable assurance that the benefits to patients outweigh the risks. While the increased use of wireless technology and software in medical devices also increases the risks of potential cybersecurity threats, these same features also improve health care and increase the ability of health care providers to treat patients.

Addressing cybersecurity threats, and thus reducing information security risks.



**Content of Premarket Submissions for Management of Cybersecurity in Medical Devices**

**Guidance for Industry and Food and Drug Administration Staff**

Document Issued on: October 2, 2014

The draft of this document was issued on June 14, 2013.

**FDA FACT SHEET**

**THE FDA'S ROLE IN MEDICAL DEVICE CYBERSECURITY**  
*Dispelling Myths and Understanding Facts*

As medical devices become more digitally interconnected and interoperable, they can improve the care patients receive and create efficiencies in the health care system. Medical devices, like computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. By carefully considering possible cybersecurity risks while designing medical devices, and having a plan to manage emerging cybersecurity risks, manufacturers can reduce cybersecurity risks posed to devices and patients.

The FDA has published premarket and postmarket guidances that offer recommendations for comprehensive management of medical device cybersecurity risks, continuous improvement throughout the total product life-cycle, and incentivize changing marketed and distributed medical devices to reduce risk. Even with these guidances, the FDA continues to address myths about medical device cybersecurity.

Dispelling the Myths	Understanding the 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.
Cybersecurity for medical devices is optional.	Medical device manufacturers must comply with federal regulations. Part of those regulations, called quality system regulations (QSRs), requires that medical device manufacturers address all risks including cybersecurity risk. The pre- and post-market cybersecurity guidances provide recommendations for meeting QSRs.
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

For questions regarding this document contact the Office of Communication, Outreach and Development (OCOD)

Center for Devices and Radiological Health  
**CDRH**

**CBER**

*Contains Nonbinding Recommendations*

**Postmarket Management of Cybersecurity in Medical Devices**

**Guidance for Industry and Food and Drug Administration Staff**

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or [ocod@fda.hhs.gov](mailto:ocod@fda.hhs.gov).

# Key Principles of FDA Premarket Cybersecurity Guidance

- Shared responsibility between stakeholders, including healthcare facilities, patients, providers, and manufacturers of medical devices
- Address cybersecurity during the design and development of the medical device
- Establish design inputs for devices related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g)





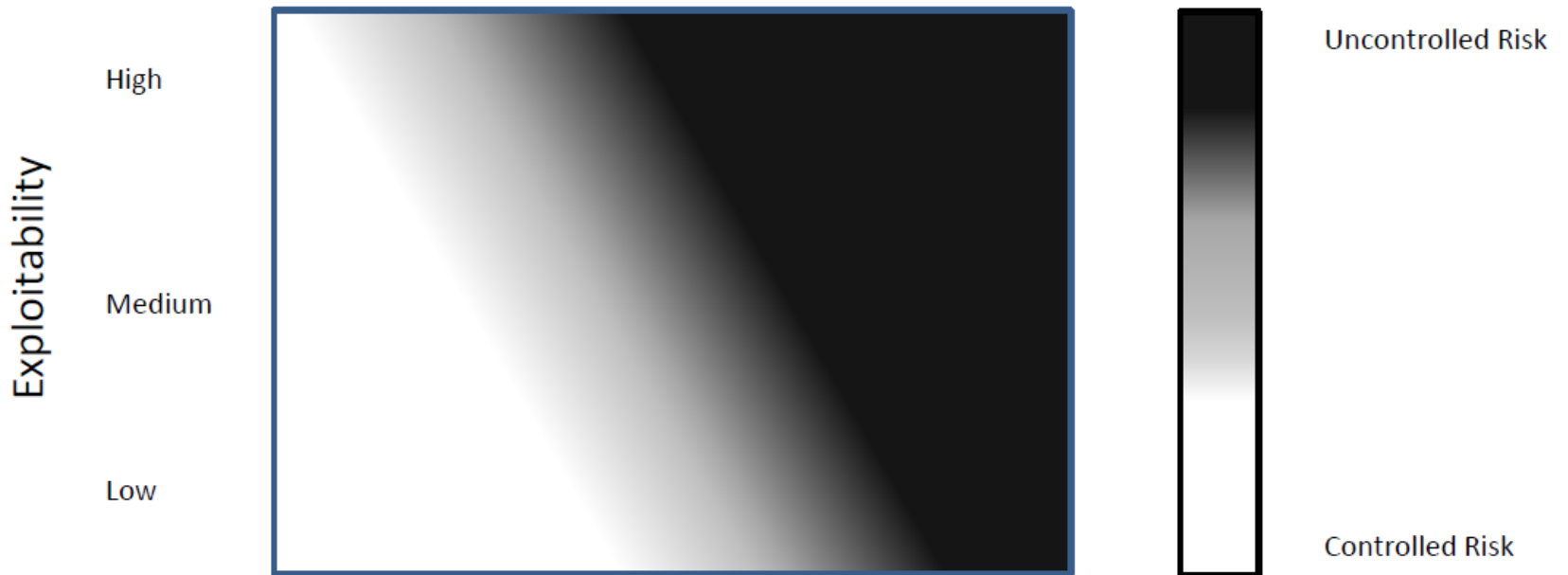
# Key Principles of FDA Postmarket Management of Cybersecurity in Medical Devices

- Use a risk-based framework to assure risks to public health are addressed in a continual and timely fashion
- Articulate manufacturer responsibilities by leveraging existing Quality System Regulation and postmarket authorities
- Foster a collaborative and coordinated approach to information sharing and risk assessment
- Align with Presidential EOs and NIST Framework
- Incentivize the “right” behavior

# Postmarket Cybersecurity Risk Assessment

Severity of Patient Harm (if exploited)

Negligible    Minor    Serious    Critical    Catastrophic



# Lessons Learned—Evolving Our Thinking

- Coordinated vs. non-coordinated disclosure of device vulnerabilities
  - Ability to get to ground truth as fast as possible so that mitigations can be proactively communicated and executed in a timely manner
    - JnJ Animas Insulin Pump
  - Non-coordinated disclosure results in delayed assessments, communications, and mitigations
    - St Jude/Abbott pacemakers and ICDs
- Impact on HPH critical infrastructure and potential disruption of clinical care
  - Patching operating system is not routine with safety-critical systems
    - WannaCry Global Cyber Attack (May 2017)
    - Petya/notPetya (July 2017)
  - Delays in diagnosis/treatment intervention can result in patient harm too
- Potential for remote, multi-patient (i.e., scaled) attack of highest concern for harm



# Medical Device Safety Action Plan:

## *Advancing Medical Device Cybersecurity*

- Update premarket cybersecurity guidance
- Consider seeking additional premarket and postmarket authorities to:
  - Require that firms build capabilities to update and patch device security into a product’s design and to include appropriate data supporting this capability in premarket submissions to FDA
  - Require firms to develop a “Software Bill of Materials” (SBOM) and to share with customers
  - Require that firms adopt policies and procedures for coordinated disclosure of vulnerabilities as they are identified
- President’s FY 2019 Budget proposes appropriations to help establish a CyberMed Safety (Expert) Analysis Board (CYMSAB) functioning as a public-private model, and serving the ecosystem as a neutral entity; also proposes appropriations to support FDA device cybersecurity capabilities

# Current FDA Efforts

- Update medical device cybersecurity premarket guidance
  - Address subset of devices for which potential of harm resulting from remote, multi-patient attack exists
  - Address subset of connected devices for which lack of availability (functionality disabled or manipulated) may result in disruption to clinical care, causing potential for harm
- Cybersecurity preparedness and incident response (MITRE collaboration)
  - Test plans containing a set of realistic testing scenarios for medical devices in the clinical environment to help foster regional and national preparedness
  - Develop preparedness and response “playbooks” for FDA and third parties
    - FDA Medical Device Cybersecurity Preparedness and Response Playbook
    - Regional Preparedness and Response Playbook for Medical Device Cyber Resilience
  - Support development of sandbox for clinical simulation and testing in safe space
  - Develop MOUs with emerging ISAOs to enhance information-sharing, with an emphasis on information relevant to patient safety and treatment

*(Cont'd)*

# Current FDA Efforts

- Create clinical rubric for Common Vulnerability Scoring System (CVSS) as medical device development tool (MDDT)
- Co-lead public-private sector stakeholder engagement in SBOM workstream
- Initiate CYMSAB pilot by engaging our stakeholders on potential models and operating structures
- Participate in Medical Device Innovation Consortium's development of a playbook for coordinated vulnerability disclosures
- Review and evaluate legislative proposals that catalyze and accelerate progress

# Cross-Agency Collaborative Efforts

- Cybersecurity Working Groups
  - CDRH Cybersecurity Working Group coordinates and collaborates with Department colleagues, including the HHS Cybersecurity Working Group, in response to medical device cybersecurity incidents and other activities
- Healthcare Sector Coordinating Council
  - FDA contributed subject matter expertise to the Healthcare Industry Cybersecurity Task Force in development of the report issued in June 2017
  - FDA taking the lead on implementation of Imperative No. 2, “Increase the security and resilience of medical devices and health IT”
- Coordination with DHS
  - Routine coordination in which FDA provides clinical subject matter expertise to evaluate and respond to potential cybersecurity vulnerabilities and/or incidents involving medical devices
  - Currently discussing execution of Memorandum of Agreement to formalize information-sharing processes

