Health Sector Coordinating Council
Cybersecurity Working Group

Secure Medtech

Health Industry Cybersecurity -

Medical Device and Health IT Joint Security Plan Version 2.0

MARCH 2024

A Joint Security Plan for medical device manufacturers and healthcare information technology cybersecurity to:

- Promote transparency on security of products
- Provide consistent secure product development practices
- Clarify vulnerability communication and incident response coordination
- Address risk of end-of-life and legacy products
- Assess maturity and establish milestones for achieving success
- Create governance structure for continuous improvement

The JSP represents a consensus based Total Product Lifecycle (TPLC) reference guide for **developing**, **deploying**, and **supporting** cyber-secure technology solutions in the healthcare environment.

Written with involvement of stakeholders **across the healthcare ecosystem** and intends to reflect **"joint" expectations** of what a mature product security capability should look like for medical technology.

The JSP is a significant step toward the Health Industry Cybersecurity Strategic Plan (HIC-SP) goal #6 which states *"Healthcare technology used inside and outside of the organizational boundaries is secure-by-design and secure-by-default while reducing the burden and cost on technology users to maintain an effective security posture."*

Written with involvement of stakeholders across the healthcare ecosystem from public and private sector stakeholders including medical device manufacturers, healthcare IT vendors, healthcare providers, and federal agencies under the umbrella of the Healthcare and Public Health Sector Coordinating Council (HSCC) Joint Cybersecurity Working Group (JCWG).

Acknowledgement to regulators and industry groups that contributed to JSP 2.0

FDA
Medtronic
OLYMPUS
Boston Scientific
Alcon
crothall healthcare
The premier healthcare support service provider nationwide
PHILIPS
SIEMENS Healthineers
MDIC Medical Device Innovation Consortium
BD
Baxter
Abbott
GE HealthCare
LivaNova
Health innovation that matters
MedSec
Edwards Lifesciences
BRACCO MEDICAL TECHNOLOGIES
werfen
INTUITIVE SURGICAL®
VELENTIUM
Medcrypt
Deloitte.
Level Nine
SublettConsulting
apraciti
cybersecurity for medtech
leidos
UL

Medical device cybersecurity landscape

2014
- FDA Guidance for Pre-Market Submissions

2015

2016
- FDA Guidance for Post-Market Submissions
- AAMI TIR 57: 2016 Principles for medical device security (pre-market)

2017

2018
- FDA Draft guidance - Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

2019
- Health Sector Coordinating Council Cybersecurity Working Group
  - HSCC Joint Security Plan
  - HHS and HSCC Release Voluntary Cybersecurity Practices for the Health Industry
- AAMI TIR 97: 2019 Principles for medical device security (post market)

2020

2021
- EU MDR

2022
- Health Sector Coordinating Council Cybersecurity Working Group
  - Operational Continuity-Cyber Incident Checklist
  - MedTech Vulnerability Communications Toolkit
  - Model Contract-Language for Medtech Cybersecurity
- IMDRF International Medical Device Regulators Forum

2023
- FDA Final guidance - Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submission
- Health Sector Coordinating Council Cybersecurity Working Group
  - Health Industry Cybersecurity Information Sharing Best Practices (HIC-ISBP)
  - Coordinated Healthcare Incident Response Plan
- U.S. Security and Exchange Commission

2024
- Health Sector Coordinating Council Cybersecurity Working Group
  - Health Industry Cybersecurity Strategic Pla
  - **HSCC Joint Security Plan 2.0**

2025

2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025

Other global industry frameworks and guidance released in parallel

JSP 2.0 Highlights

Not intended to be a complete rewrite, but rather integration of useful resources and clarification of the framework to make this a more useful tool for medical technology providers, regardless of size and scale.

Updated standards

Increased integration of external standards and guidance into relevant activities. This supports easy referencing to find additional supporting information as the JSP is leveraged to mature product security capabilities.

Refreshed framework

Refreshed framework and diagram to drive clarity and consistency. Specifically, framework components were updated to be “activities” in a secure product development framework and aligned to supporting content describing those activities.

Applied learnings

Applied learnings and improvements identified from the MDIC Medical Device Cybersecurity Maturity: Industry Benchmarking Report 2022, as well as a review from the HSCC conducted by a cross-industry group of manufacturers, HDOs, and regulators.

Concept Phase

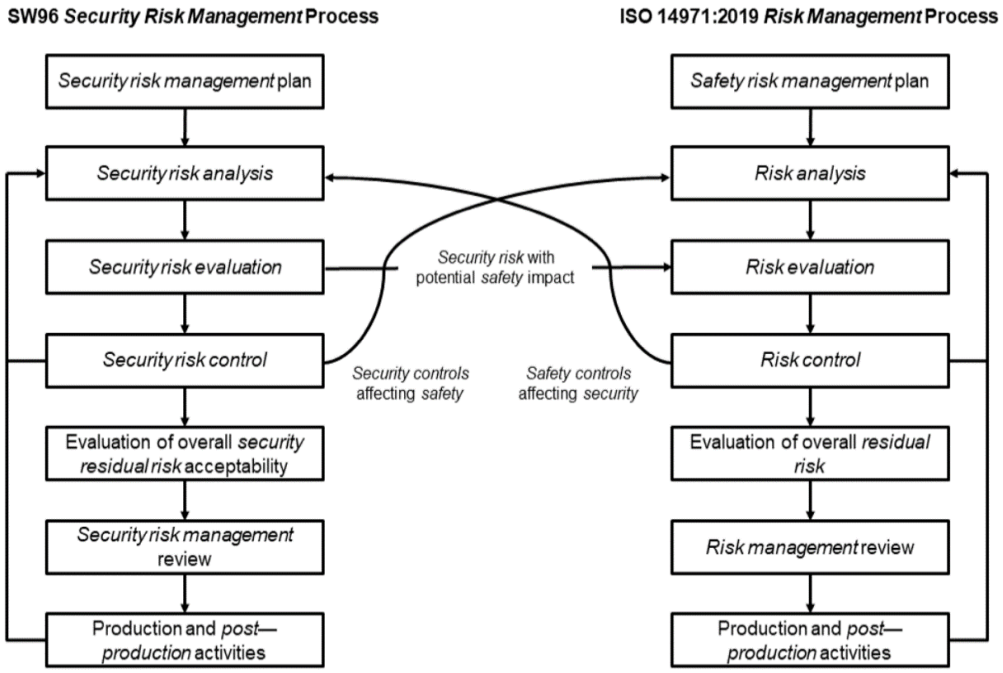
Planning for and managing potential security risk in this phase is essential

- Effectively planning for and managing potential security risk in this phase is essential to ensuring adequate resourcing and planning throughout development efforts.
  - *Failure to adequately consider security risk in this phase can result in lack of resources, both financial and human, required to ensure adequate security is built into the product.*
- At this point in development, security can be introduced early on to address potential risks introduced by the scope of the current project.

Risk Management

Security risk management is an integral component of overall product risk management

- Focuses on considerations for cybersecurit risks identified during design, development, or post launch are analyzed, evaluated, and controlled to adequately reduce and document acceptable residual risk, i.e. AAMI SW96:2023.
- This includes security risk management activities from product concept through end of support.



Security Design Risk Assessment
Security Integration into Safety Risk Assessment

Security Risk Management Summary Approval

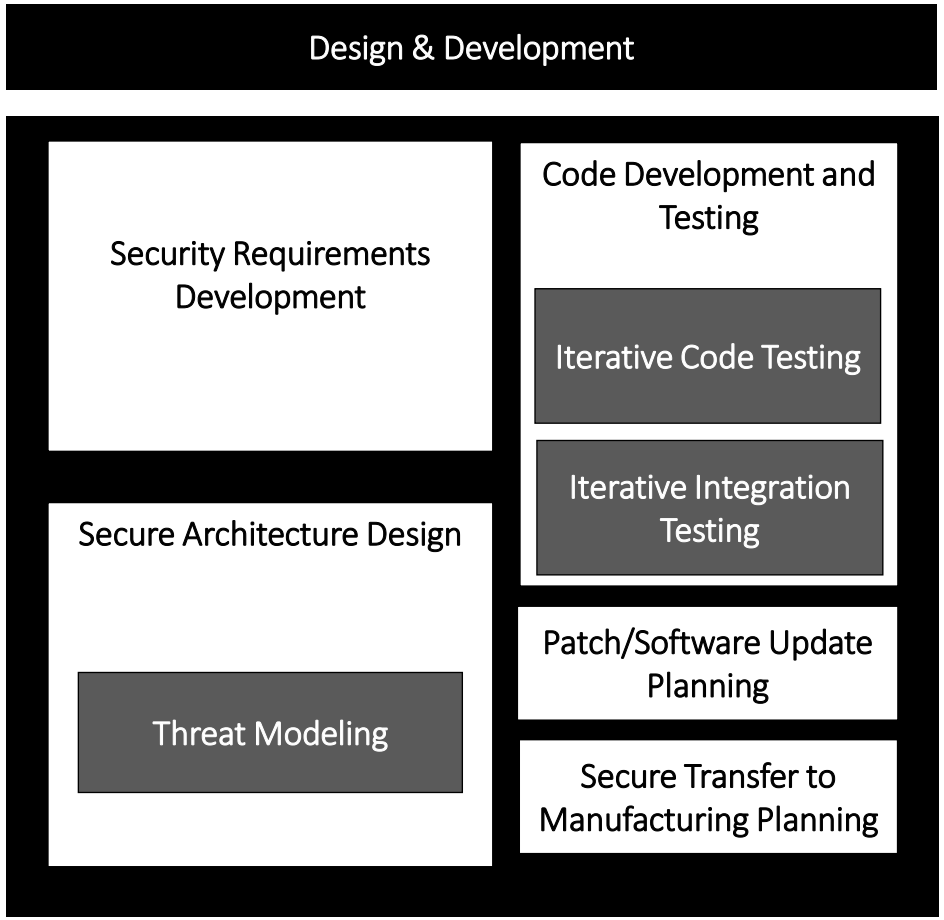
Supplier Management

Suppliers include contracted developers or service providers, hardware and software supplier, and open-source library

- Manufacturers should have procedures that include security risk management that are leveraged to evaluate, contract, and manage performance of prioritized suppliers
- This include process for managing security risk exposures, threats, and vulnerabilities throughout the supply chain as well as developing strategies to respond to the risks presented by the supplier, the supplied products and services, or the supply chain.

Design & Development

Security risk management is an integral component of overall product risk management



- Establishes detailed specifications for a product, including implementation, design controls, design inputs and design outputs
- This includes clear outlining of critical activities that shall take place during development such as architecture reviews, threat modeling and iterative testing and secure transfer to manufacturing.

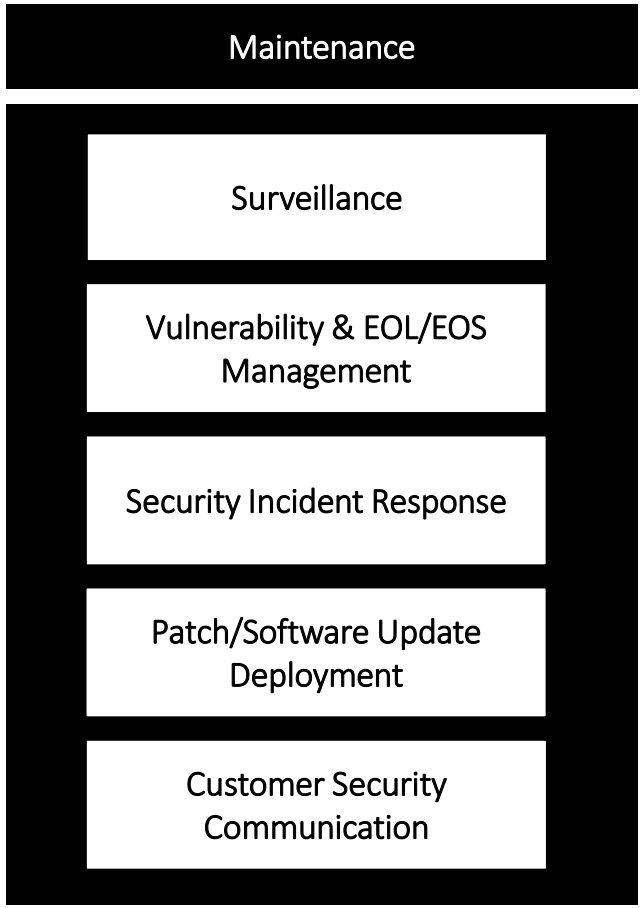
Verification & Validation

Diverse testing activities based on their objective, involved tools, skillsets, and discrete outcomes.

- Decomposes cybersecurity testing into the discrete activities that may occur during the Verification & Validation stage of Design & Development.
- Formally defining the purpose and output of each activity further enables the creation of mature cybersecurity engagement processes and automation

Maintenance

Essential capabilities to maintain the security of products over their lifecycle.



- These processes should generate records that demonstrate that activities are being effectively executed to ensure maintenance of products, including incident response.
- Manufacturers should provide timely responses and communications to all stakeholders impacted by exploited vulnerabilities and security incidents for commercialized products

Evaluating JSP Progress and Maturity

Benchmarking will support potential needed investments and help industry on sector progress

Performing a periodic maturity assessment against the JSP can provide organizations valuable input when determining where product security risks and potential program investments may be required

MDIC annually collects shared results and produces a report on overall industry progress. This report is invaluable both to organizations to benchmark themselves as well as to inform industry efforts on where more support on security product development activities may be required.
https://mdic.org/program/cybersecurity/

HEALTH SECTOR COORDINATING COUNCIL
Cybersecurity Working Group

Greg Garcia
Executive Director
Greg.Garcia@HealthSectorCouncil.org

Allison Burke
Member Engagement Project Manager
Allison.Burke@HealthSectorCouncil.org

Morgan Shuey
Member Support Intern
Morgan.Shuey@HealthSectorCouncil.org

https://HealthSectorCouncil.org