Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

Health Industry Cybersecurity –

Managing Legacy Technology Security (HIC-MaLTS)

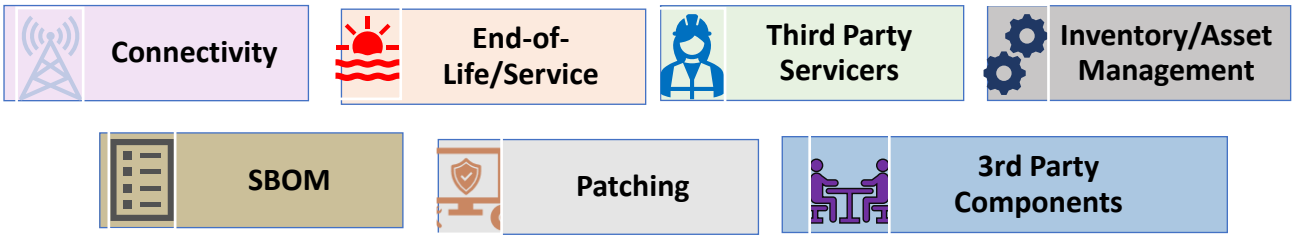
What is it? – The Health Industry Cybersecurity – Managing Legacy Technology Security (HIC-MaLTS) is a comprehensive resource – organized in modular, actionable components - for the management of cyber risk caused by legacy technologies used in healthcare environments. It recommends cybersecurity strategies that both manufacturers and health providers can implement for legacy medical technology as a shared responsibility in the clinical environment, and provides insights for designing future devices that are more secure.

Who should use it? – The HIC-MaLTS details best practices and recommendations for medical device manufacturers (MDMs), healthcare delivery organizations (HDOs), and other technology providers whose products are used in healthcare environments.

What does it cover? – HIC-MaLTS covers, among other things:

- The "Core Pillars" of a comprehensive legacy technology cyber risk management program:
  - **Governance:** How should healthcare stakeholders govern to ensure effective legacy technology cyber risk management?
  - **Communications:** Internally, to their customers, regulators, and the public—how should organizations communicate to manage legacy technology risk?
  - **Cyber Risk Management:** For current and future legacy technologies, how should organizations manage cyber risk to limit current risk and avoid or minimize future risk?
  - **Future Proofing:** How should MDMs and other technology providers design, deploy, and maintain their technologies to avoid or lessen legacy technology risks?

- Common legacy risk management **challenges, and recommendations** for addressing them, including:



Highlighted Sections

Responsibility Transfer Framework

- For financial, logistical, and operational reasons, HDOs may consider continuing to use legacy technologies even after support is discontinued
- The **Responsibility Transfer Framework** details important factors HDOs should assess to make an informed decision about the potential risks of doing so
- The Framework examines factors related to: (1) safety and effectiveness, (2) clincial impacts, and (3) techncial risk management

Patching Lifecycle Recommendations

- Patching remains a major cyber risk management activity, but is also a major challenge
- The **Patching Lifecycle Recommendations** section breaks down the patching lifecycle from first identifying an issue that may need patching (signal identification), to patch development, to patch installation and testing
- Includes recommendations tailored to each lifecycle stage

Future Proofing (including Software and Vendor Selection)

- Designing technologies to *avoid and minimize* future legacy pressures is as important as managing current legacy technologies
- The **Future Proofing** section details recommendations for designing, deploying, and maintaining technologies to extend the product lifecycle and mitigate future legacy issues
- Includes discussion of (1) threat modeling practices, (2) technology design (including software and vendor selection), and (3) facilitating secure technology deployment