Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Medical Device and Health I.T. Joint Security Plan
Frequently Asked Questions

Q1: **How can medical technology companies get more help implementing these recommendations?**

A: A supplemental infographic is provided by the Healthcare Sector Coordinating Council on their website (www.healthsectorcouncil.org). In addition, webinars will be provided to review specific sections of the JSP.

Q2: **How will you measure improvement in the security of medical technology? What organizations will be measuring implementation?**

A: There is a specific section in the JSP that describes how to evaluate maturity against the JSP. In particular, there are specific questions related to JSP content that can be used to determine maturity levels (according to CMMI).

Q3: **How does this joint security plan relate to other medical technology security standards or guidelines?**

A: The JSP is not a standard, it is a unifying plan which medical technology companies can voluntarily commit to and healthcare providers can request from their vendors. The framework and components of the JSP are sourced from a number of authoritative sources for best practice in security.

Q4: **Have any companies committed to testing the guidelines on their own operations? What were the results?**

A: The latest version of the JSP is reflective of multiple review periods with medical technology companies, healthcare providers, trade associations, security researchers, and regulators. Several large and small medical technology companies have piloted the JSP. The responses and feedback were overwhelmingly positive.

Q5: **How will this help hospitals improve the security of their operations when purchasing and deploying medical devices?**

A: The JSP will help hospitals in several ways. One is that as hospitals purchase and deploy products that are developed “secure by design”, the cyber vulnerability of those devices and the related institutional risk are significantly reduced, resulting in lower risk to patient safety. A second improvement is that, given the expense and complexity of mitigating many medical devices risks, having a “secure” device can lower a HDO’s security costs and complexity. A third benefit is providing visibility to the devices that are on the network. Knowing what software is running, what vulnerabilities might be present and other basic information allows hospitals to be proactive in implementing any additional controls or monitoring.

Q6: **Does the provider community support this approach?**

A: Healthcare providers contributed to and support the JSP's approach to this shared responsibility. They understand that it takes everyone in the device lifecycle to keep their facility and patients safe. This includes regulatory bodies, vendors, resellers, and local healthcare facilities.

Q7: **Will FDA be measuring adoption of these guidelines for regulatory purposes?**

A: The JSP is not a regulatory document. It is a consensus-based total product lifecycle reference guide for developing, deploying, and supporting cyber secure technology solutions in the health care environment. Recognizing that medical device cybersecurity is a shared responsibility, FDA encourages collaborations like this which seek to proactively address cybersecurity challenges.

Q8: **What is the HSCC and who came up with these guidelines?**

A: The HSCC is an industry-driven public private partnership of healthcare companies and providers developing collaborative solutions to mitigate threats to critical healthcare infrastructure. It is one of 16 critical infrastructure sectors organized to partner with the government under Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience. The JSP task group was co-chaired by Becton Dickinson, Mayo Clinic and the FDA under the auspices of the HSCC Joint Cybersecurity Working Group, which includes more than 200 medical device and health IT companies, direct patient care entities, plans and payers, labs, blood and pharmaceutical companies.

Q9: **How do we provide feedback on the tool?**

A: To provide feedback on this tool, please send comments to: JSPFeedback@HealthSectorCouncil.org

##

***Contact**: Greg Garcia, HSCC Executive Director for Cybersecurity*
Greg.Garcia@HealthSectorCouncil.org