We appreciate the opportunity to respond to “Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management” RFI. After reviewing the project description, we believe that MedCrypt would be a valuable part of the reference architecture as we offer solutions that operationalize the complex problems of software bill of materials (SBOM) and vulnerability management. While a subset of the scope of the problem, we need to recognize the complexity challenges of solving for this and therefore these are critical and our solutions both automate and integrate to scale across the entire value chain.

Why: Our solution enables medical device manufacturers to overcome challenges around scaling, efficiency, and on-going support over the lifetime of a device.

Who: We are committed to collaborating with the various project participants. Where needed, our team can support interface, connectivity, set-up, instructions, and script support necessary to demonstrate the desired MedCrypt capabilities.

How: In the table below, we have outlined how our solution will address the specific requirements laid out in the project description.

I look forward to further discussing our participation in the project and ultimate inclusion in improving NIST cybersecurity resources.

Sincerely,
The MedCrypt Team ([redacted])

Understanding of the Project:
Our solution has taken special consideration for scaling vulnerability management in software after the product is out in the field. We’ve focused on healthcare as the use-case for vulnerability management post-market is fundamentally different from pre-market.

Our Relevance to Topics in Scope:

The table below outlines the overlap of Functions and Solution Characteristics where MedCrypt would have an impact:

Cybersecurity Supply Chain Risk Management Topic in RFI	**Medcrypt Functionality**
11. National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?	Greatest challenges are: ● Continuous visibility and maintenance over the lifetime of a product ● Visibility across stakeholders at various points in device lifecycle (e.g. product security takes over this management after engineering build the product) ● For healthcare, integration into ‘how’ devices are developed - i.e.

	Quality Management System (QMS) based requirements across a products Secure Development Lifecycle (SDLC)
12. Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (e.g. pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.	● Our SBOM and vulnerability management tool (Heimdall) provides machine readable format for SBOM generation and consumption for sharing between producer and consumer ● We have automated the software component to vulnerability matching process
13. Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider to achieve greater assurance throughout the software supply chain, including for open-source software?	● Communication protocol from medical device manufacturer to healthcare delivery organization is not standardized ● Our solution provides for automated exchange of vulnerability data across stakeholders
14. Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.	Our solution was developed in compliance with established standards (NIST SP 800-161), guidances (e.g., FDA pre- and post-market guidance), and frameworks (e.g., NIST CSF)