Medical Device Innovation Consortium
www.mdic.org

RFP Posting: April 13, 2018
Indication of Interest: April 27, 2018
Proposal Due: May 4, 2108

Medical Device Innovation Consortium (MDIC)

Cybersecurity in the Medical Device Sector: Coordinated Vulnerability Reporting

Request for Proposals (RFP)

The Medical Device Innovation Consortium (MDIC) is seeking a contractor to synthesize case studies and learnings from medical device companies that have implemented vulnerability reporting portals and processes into a final report and presentation at the MDIC Annual Public Forum.

Background

MDIC recognizes that cybersecurity is critical infrastructure vital to the United States. Cybersecurity threats can have a debilitating effect on security, national economic security, and national public health or safety. As such, MDIC is focused on making meaningful contributions to advance cybersecurity as it relates to medical devices.

The U.S. Food and Drug Administration's (FDA) Center for Devices and Radiological Health (CDRH) has issued guidance to address cybersecurity as part of their ongoing effort to ensure safety and effectiveness of medical devices across their lifecycle. It is recommended manufacturers build risk management programs that span premarket from early design, through development of products, and into the postmarket environment. [1, 2]

Some medical device manufacturers have implemented coordinated cybersecurity vulnerability portals and processes as one tool in their overall threat detection and response process. These portals and processes enable manufacturers to receive findings from researchers regarding potential vulnerabilities in a device. However, the majority of medical device manufacturers do not have portals or defined processes to receive these findings and to act on this information in a timely way. MDIC believes that coordinated cybersecurity vulnerability processes and portals are integral to a comprehensive approach to counteract cybersecurity threats.

About MDIC

The Medical Device Innovation Consortium (MDIC) is the first public-private partnership created with the sole objective of advancing medical device regulatory science throughout the total product life cycle. MDIC's mission is to promote public health through science and technology and to enhance trust and confidence among stakeholders. We work in the pre-competitive space to facilitate development of methods, tools, and approaches that enhance understanding and improve evaluation of product safety, quality, and effectiveness. Tools and methods are made available to the public to benefit the broader

[1] Reference FDA Guidance, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. October 2, 2014.
[2] Reference FDA Guidance, Postmarket Management of Cybersecurity in Medical Devices. December 28, 2016.

medical device and healthcare ecosystem. Our initiatives improve product safety and patient access to cutting-edge medical technology while reducing cost and time to market.

More information on MDIC is available at: http://www.mdic.org

Project Concept and Ownership

The goal of this RFP is to identify a contractor to interview medical device companies and synthesize information and case studies on vulnerability reporting portals and processes into a report format that will serve as a "playbook" for medical device companies interested in establishing their own cybersecurity portal systems. All information developed through this project, including during the RFP process, will be owned by MDIC.

MDIC's Role

MDIC staff will oversee the management of this project and provide approval for any interim and final deliverables.

Details and Requirements

Proposals should specify a plan for developing a medical device company cybersecurity portal playbook to address the following three sections.

A. A research plan designed and conducted to address - and not limit to - the following questions:
   1. What coordinated cybersecurity vulnerability portals and processes are used today, both in the medical device industry and in other industries?
      a. What do they look like?
      b. How do they operate?
   2. What practices surrounding coordinated cybersecurity vulnerability portals and processes have worked for our member companies? Which of these best practices should be duplicated in future efforts by other medical device manufacturers?
   3. What are the legal, regulatory, and business risks associated with coordinated cybersecurity vulnerability portals and processes?
   4. What measures are used to determine effectiveness of coordinated cybersecurity vulnerability portals and processes?
   5. What are the benefits of use of coordinated cybersecurity vulnerability portals and processes?
   6. How is information populated within the cybersecurity vulnerability portal and how is it acted upon?
      a. How are incidence reports prioritized within the portals?
      b. How are reports processed (e.g., how reviewed, decision-making process, closed loop reporting, escalation, roles/responsibilities, external reporting)
      c. What are the actions that your organization may take based on information received in the portal?
   7. How do organizations with coordinated cybersecurity vulnerability portals and processes obtain organizational buy-in surrounding the introduction and implementation of the portals and processes? What are the barriers and challenges?

B. The plan should include synthesizing this research and delivering a final report ("playbook"). While cybersecurity risk management systems may not be considered competitive, the plan should include an approach that maintains applicable confidentiality of interview/survey respondents and companies.

C. The plan should include a timeline and outlined deliverables (see below) and presenting the results of the work at the MDIC Annual Public Forum (MAPF), scheduled for September 5, 2018.

Submission Components

To enable MDIC to evaluate the submission, the responding proposal must include the following:

- A plan for developing cybersecurity vulnerability reporting portal system (portal and processes) playbook for medical device companies
- The proposal must comply with the guidelines outlined above and **not exceed 10 pages**
- A timeline for completing the required deliverables **by and at the MAPF scheduled for September 5, 2018**
- A proposed budget
- A proposed project team and curriculum vitae (CVs) of potential team members
- Experience summary: what similar projects have you conducted (describe without disclosing confidential information)

MDIC encourages interested parties to arrange a teleconference with MDIC to discuss potential submissions.

Confidentiality

MDIC operates in a dynamic business environment. Throughout this RFP process, respondents will gain access to information considered confidential by Members of the Consortium. The confidential information includes this RFP, and all information and materials relating to the business and processes of the Consortium. MDIC requires that respondents will maintain confidentially of all such information. Only MDIC shall have the right to release any publicity concerning this RFP.

Period of Performance

June 4, 2018 (work initiation) – September 5, 2018

Deliverables to be completed within the period of performance

MDIC staff will approve each of the following deliverables and interim deliverables. These deliverables represent a minimum set of required deliverables. Additional deliverables can be proposed within the application.

Deliverable	Associated Interim Deliverables
1. Research plan, data collection techniques, and identification of data sources	a. Draft plan (RFP) b. Final plan
2. Cybersecurity portal system (vulnerability reporting portals and processes) playbook	a. Outline of playbook b. Draft playbook c. Final playbook

3. Presentation at MDIC Annual Public Forum (MAPF)	a. Draft presentation materials b. MAPF presentation September 5, 2018

Review Process

Responses to this RFP will be reviewed by MDIC staff. MDIC staff reserve the right to contact applicants with additional questions during the review period. MDIC staff reserve the right to consult any MDIC member organizations during the review and evaluation of RFP process. Responses will be reviewed for completeness and appropriateness of the responses as they pertain to the required submission components. MDIC will consider both the programmatic aspects of the proposal, as well as the anticipated cost with the programmatic elements of the proposal receiving greater weight. MDIC may, for example, choose a costlier proposal if its programmatic offering warrants the premium. However, as potential contractors' programmatic offerings move toward equivalency, cost will gain in importance.

MDIC's selection of a contractor will be contingent on the parties executing a mutually acceptable contract on or before June 4, 2018. MDIC reserves the right to terminate contract negotiations at any time and select another contractor if it determines that it is unlikely that an agreement will be executed in a timely manner.

Timeline (projected)

- Posting Date: April 13, 2018
- Indication of interest: April 27, 2018
- Proposals Due to MDIC by 5:00 pm EST: May 4, 2018
- Notification of Selection by MDIC and Commencement of Contract Negotiations: May 11, 2018
- Work Initiated: June 4, 2018
- Work Completed: final presentation at MDIC Annual Public Conference September 5, 2018

Contact for RFP:

Please send questions, indication of interest, and proposals to Lisa Griffin Vincent, vice president (acting), Regulatory Science, MDIC: lgriffinvincent@mdic.org