Mercury to Bring Raytheon's Advanced Cyber Resiliency and Intrusion Detection Tools to the Mercury Processing Platform

Oct 9, 2023 at 7:00 AM EDT

ANDOVER, Mass., Oct. 09, 2023 (GLOBE NEWSWIRE) -- Mercury Systems, Inc. (NASDAQ: MRCY, www.mrcy.com), a technology company that delivers processing power for the most demanding aerospace and defense missions, today announced it is working with Raytheon, an RTX business, to increase survivability and resiliency of its mission-critical solutions by incorporating Raytheon's advanced cyber resiliency and intrusion detection tools into Mercury's processing platform.

As threats against critical systems continue to grow in scope and sophistication, Mercury and Raytheon recognize the need for significantly stronger security controls to protect mission-critical systems, and both are dedicated to delivering comprehensive and resilient protection solutions to maintain mission effectiveness in cyber-contested environments.

Through this relationship, Mercury gains the ability to integrate Raytheon's Electronic Armor and CADS products into its portfolio of mission systems, including secure mission processors, communication management units, rugged servers, communication management units, and data recorders. Raytheon's cybersecurity tools complement Mercury's BuiltSECURE technology that protects critical data with industry-leading physical security, cryptography, and secure boot features. Mercury and Raytheon are industry leaders in building and securing high-performance, open-architecture products and subsystems for the aerospace and defense industry, including SOSA-aligned mission computers. Their combined offerings provide aerospace and defense programs with an effective approach to addressing emerging cyber survivability endorsement requirements, which are focused on preventing, detecting, responding, and recovering from cyberattacks.

Electronic Armor is a cyber resiliency solution that prevents reverse engineering and protects the confidentiality and integrity of data, as well as applications from attackers who have bypassed traditional information assurance controls and/or gained escalated privilege on a system. Among its many features is the hardening of the operating system, providing data-at-rest and runtime protections, preventing execution of unauthorized applications, and preventing modification/introspection of sensitive applications and data.

CADS is a real-time Intrusion Detection System (IDS) for the standard control buses found in airframes and ground vehicles. CADS provides cyber anomaly detection and complete bus traffic logging for mission- and safety-critical systems. It heightens situational awareness for platform operators and support teams and includes offline analysis tools to provide long-term performance and cross-fleet analysis of cyber trends.

To learn more about how Raytheon's Electronic Armor and CADS solutions can integrate with Mercury hardware, visit the Mercury booth (#1439) at this week's AUSA Annual Meeting and Exposition.

Mercury Systems – Innovation that matters®
Mercury Systems is a technology company that pushes processing power to the tactical edge, making the latest commercial technologies profoundly more accessible for today's most challenging aerospace and defense missions. From silicon to system scale, Mercury enables customers to accelerate innovation and turn data into decision superiority. Mercury is headquartered in Andover, Massachusetts, and has 24 locations worldwide. To learn more, visit mrcy.com. (Nasdaq: MRCY)

Forward-Looking Safe Harbor Statement
This press release contains certain forward-looking statements, as that term is defined in the Private Securities Litigation Reform Act of 1995, including those relating to the Company's focus on enhanced execution of the Company's strategic plan under a refreshed Board and leadership team. You can identify these statements by the words "may," "will," "could," "should," "would," "plans," "expects," "anticipates," "continue," "estimate," "project," "intend," "likely," "forecast," "probable," "potential," and similar expressions. These forward-looking statements involve risks and uncertainties that could cause actual results to differ materially from those projected or anticipated. Such risks and uncertainties include, but are not limited to, continued funding of defense programs, the timing and amounts of such funding, general economic and business conditions, including unforeseen weakness in the Company's markets, effects of any U.S. federal government shutdown or extended continuing resolution, effects of geopolitical unrest and regional conflicts, competition, changes in technology and methods of marketing, delays in or cost increases related to completing development, engineering and manufacturing programs, changes in customer order patterns, changes in product mix, continued success in technological advances and delivering technological innovations, changes in, or in the U.S. government's interpretation of, federal export control or procurement rules and regulations, changes in, or in the interpretation or enforcement of, environmental rules and regulations, market acceptance of the Company's products, shortages in or delays in receiving components, supply chain delays or volatility for critical components such as semiconductors, production delays or unanticipated expenses including due to quality issues or manufacturing execution issues, failure to achieve or maintain manufacturing quality certifications, such as AS9100, the impact of the COVID pandemic and supply chain disruption, inflation and labor shortages, among other things, on program execution and the resulting effect on customer satisfaction, inability to fully realize the expected benefits from acquisitions, restructurings, and execution excellence initiatives or delays in realizing such benefits, challenges in integrating acquired businesses and achieving anticipated synergies, effects of shareholder activism, increases in interest rates, changes to industrial security and cyber-security regulations and requirements and impacts from any cyber or insider threat events, changes in tax rates or tax regulations, such as the deductibility of internal research and development, changes to interest rate swaps or other cash flow hedging arrangements, changes to generally accepted accounting principles, difficulties in retaining key employees and customers, which difficulties may be impacted by the termination of the Company's announced strategic review initiative, unanticipated challenges with the transition of the Company's Chief Executive Officer and Chief Financial Officer roles, including any dispute arising with the former CEO over his resignation, unanticipated costs under fixed-price service and system integration engagements, and various other factors beyond our control. These risks and uncertainties also include such additional risk factors as are discussed in the Company's filings with the U.S. Securities and Exchange Commission, including its Annual Report on Form 10-K for the fiscal year ended June 30, 2023 and subsequent Quarterly Reports on Form 10-Q and Current Reports on Form 8-K. The Company cautions readers not to place undue reliance upon any such forward-looking statements, which speak only as of the date made. The Company undertakes no obligation to update any forward looking statement to reflect events or circumstances after the date on which such statement is made.

INVESTOR CONTACT
Nelson Erickson
Senior Vice President, Strategy and Corporate Development
Nelson.Erickson@mrcy.com

MEDIA CONTACT
Turner Brinton
Sr. Director, Corporate Communications
Turner.Brinton@mrcy.com