



Arteris Wins Funding to Expand Hardware Design Supply Chain Security Assurance for the Trusted and Assured Microelectronics Program

October 6, 2026

Government-funded initiative advances commercially sourced third-party IP security assurance for semiconductor systems used in mission-critical aerospace and defense systems

CAMPBELL, Calif., Oct. 06, 2026 (GLOBE NEWSWIRE) -- Arteris, Inc. (Nasdaq: AIP), a leading provider of semiconductor technology for accelerating innovation in the AI era, today announced the expansion of its third-party IP (3PIP) security assurance program in collaboration with BAE Systems and SiFive, Inc. This program has received an additional \$3.3 million in funding through the Trusted and Assured Microelectronics (T&AM) program within the Office of the Under Secretary of War for Research and Engineering (OUSW(R&E)).

The T&AM Program drives modernization of defense systems through access to advanced microelectronics. To support aspects of this program, this initiative brings together Arteris, BAE Systems, and SiFive to advance third-party IP security assurance methodologies for mission-critical semiconductor systems. The focus is on helping to address the growing challenge of ensuring the security and trustworthiness of commercially sourced third-party silicon IP integrated into advanced systems-on-chip (SoCs).

The expanded program builds on prior successful collaboration among the government and companies and will further enhance secure integration methodologies for third-party IP components operating within complex semiconductor systems. The collaboration also supports broader industry and government efforts to strengthen semiconductor design supply chain security. The collaboration between Arteris, BAE Systems, and SiFive is focused on establishing a repeatable, evidence-based methodology to evaluate and verify the secure implementation, integration, and usage of third-party IP integrated into SoC environments.

"Third-party commercial IP is essential to developing today's advanced semiconductor systems and maintaining the speed and innovation required for the next-generation capabilities central to BAE Systems' mission portfolio," said Joseph Lin, chief scientist at BAE Systems FAST Labs™. "The third-party IP security assurance program is pivotal in establishing practical, repeatable and measurable security assurance processes as a foundation for the timely delivery of robust and dependable mission-critical weapon systems."

"Security is a paramount priority for our RISC-V processor IP solutions, especially as RISC-V adoption accelerates across markets ranging from AI infrastructure to aerospace and defense," said John Ronco, svp of product at SiFive. "This collaboration demonstrates how the ecosystem can work together to strengthen trust in third-party IP integration and deliver practical, scalable hardware security assurance methodologies for modern semiconductor designs."

"As semiconductor supply chains become increasingly complex, third-party IP security assurance has become a critical requirement for both commercial and government applications, particularly in aerospace and defense systems, data center infrastructure, automotive platforms, and intelligent edge devices including drones and robotics," said K. Charles Janac, president and CEO of Arteris. "By collaborating with the US Government, SiFive, and BAE Systems, we are helping establish a repeatable framework for third-party IP security assurance that enables semiconductor developers to better understand, evaluate, and mitigate hardware security risks in increasingly complex semiconductor designs."

Arteris employs a Common Weakness Enumeration (CWE)-based microelectronics evidence framework that links hardware weaknesses to requirements, properties, and traceable verification evidence at a granular level. The hardware security assurance technologies from Arteris is used for coverage-oriented security evidence collection and repeatable hardware security assurance throughout the design process, from IP blocks to subsystems, chiplets, and integrated SoCs running software workloads. Learn more at arteris.com/cybersecurity.

About Arteris

Arteris is a leading provider of semiconductor technology that accelerates the creation of high-performance, power-efficient silicon with built-in safety, reliability, and security. Innovative Arteris products are designed to optimize data movement and help ease complexity in the modern AI era with network-on-chip (NoC) interconnect intellectual property (IP), system-on-chip (SoC) software for integration automation and hardware security assurance. All are used by the world's top technology companies to improve overall performance and engineering productivity, reduce risk, lower costs, and bring cutting-edge designs to market faster. Learn more at arteris.com.

About SiFive

As the pioneers who introduced RISC-V to the world, SiFive is transforming the future of computing by bringing the limitless potential of RISC-V to the highest performance and most data-intensive applications in the world. SiFive's RISC-V compute platforms have enabled leading technology companies around the world to innovate, optimize and deliver the most advanced solutions of tomorrow across every market segment of chip design, including artificial intelligence, machine learning, automotive, data center, mobile, and consumer. With SiFive, the future of RISC-V has no limits.

About BAE Systems

[BAE Systems, Inc.](https://baesystems.com) and our nearly 41,500 people are part of a global defense, aerospace, and security company with more than 110,000 employees worldwide. We design, build and deliver a full range of products and services for air, land, sea, space and cyberspace, as well as advanced electronics, intelligence, security, information technology solutions and support services. Our dedication shows in everything we do for our customers. Guided by a performance-driven culture of innovation and collaboration, our ambitious teams push the limits of possibility to protect those who protect us.

About the Trusted and Assured Microelectronics (T&AM) Program

The Trusted and Assured Microelectronics (T&AM) Program drives modernization of defense systems through access to advanced microelectronics technologies that leverage state-of-the-art, commercially driven capabilities. The program operates under the Office of the Under Secretary of War for Research and Engineering (OUSW(R&E)).

© 2004-2026 Arteris, Inc. All rights reserved worldwide. Arteris, Arteris IP, the Arteris IP logo, and the other Arteris marks found at <https://www.arteris.com/trademarks> are trademarks or registered trademarks of Arteris, Inc. or its subsidiaries. All other trademarks are the property of their respective owners.

Media Contact:

Arteris Inc.

Gina Jacobs

+1 408 560 3044

newsroom@arteris.com

This press release was published by a CLEAR® Verified individual.