EDITORIAL CONTACTS:
Microsemi Corp.
Farhad Mafie, VP Worldwide Product Marketing
949-380-6161
press@microsemi.com

The Athena Group, Inc.
Toni Sottak, Wired Island
(408) 876-4418
toni@wiredislandpr.com

Microsemi and Athena Announce FPGA Cores with Strong DPA Countermeasures for Cryptography Users

Powerful Anti-Tamper Security Microprocessor Technology Available Immediately as Soft Intellectual Property for SmartFusion2 and IGLOO2 FPGAs

ALISO VIEJO, Calif.—Oct. 13, 2015—Microsemi Corporation (Nasdaq: MSCC), a leading provider of semiconductor solutions differentiated by power, security, reliability and performance, and The Athena Group, Inc. (Athena), a leading provider of security, cryptography, anti-tamper and signal processing intellectual property (IP) cores, today announced a comprehensive portfolio of IP cores with state-of-the-art side channel analysis (SCA) and differential power analysis (DPA) countermeasures. The new portfolio, based on Athena's TeraFire® cryptographic microprocessor family, is designed for users of Microsemi's award-winning SmartFusion™2 system-on-chip (SoC) field programmable gate arrays (FPGAs) and IGLOO™2 FPGAs.

"DPA countermeasures are critical to any tamper-resistant system," said Paul Quintana, director of vertical marketing, Microsemi Defense, Security and Computing. "As threat vectors increase in sophistication, so must the security solutions. Microsemi customers are looking for the most robust and proven anti-tamper and information assurance capabilities for their products. Athena is now delivering its best-of-breed family of silicon-proven security products as soft IP for license on the industry's only DPA-resistant FPGAs certified by Rambus Cryptography Research, SmartFusion2 and IGLOO2."

Athena's robust, innovative DPA countermeasure solutions deliver resistance to side channel monitoring attacks across a broad range of standard cryptographic algorithms and performance levels used for embedded applications in markets including defense, communications and industrial. These silicon-proven cores have been recently enhanced to resist SCA/DPA attacks up to 1 billion traces and can be optimized for size, speed and security level based on customer requirements. Furthermore, since select SmartFusion2 and IGLOO2 FPGAs are the only FPGAs already licensed for Rambus Cryptography Research's DPA patent portfolio, no additional license is required from Rambus Cryptography Research for use of the Athena IP cores with the licensed Microsemi FPGAs.

"Partnering with Microsemi, a leader in highly secure, low-power FPGAs, to offer SmartFusion2 and IGLOO2 customers the most robust countermeasures available has been groundbreaking," said Stuart Audley, director of engineering at Athena. "To give Microsemi customers confidence that they are deploying IP with effective countermeasures, Athena has pushed the limits of test vector leakage assessment (TVLA) testing of our DPA solutions. We have demonstrated through measurements and statistical analysis that even after a billion traces, leakage is effectively minimized."

Microsemi's SmartFusion2 and IGLOO2 DPA-resistant FPGAs deliver design security and protection for the valuable IP embodied within users' programmable designs. While users choose SmartFusion2 and IGLOO2 for these capabilities, many users require additional cryptographic data security soft IP as part of their own programmable applications. Teaming with Athena enables users to employ sophisticated cryptographic microprocessor technology employing advanced DPA countermeasures as a soft IP, maintaining the highest levels of data security throughout the device/application operational cycle.

DPA and differential electromagnetic analysis (DEMA) are types of SCA that involve monitoring variations in the electrical power consumption or electromagnetic emissions from a target device, respectively. DPA and DEMA attacks are non-invasive, easily automated and can be mounted without knowing the design of the target device. Unlike invasive tampering, electromagnetic attacks can even be performed at a distance. As an example, electromagnetic attacks on cell phones have been demonstrated at a range of 30 feet. DPA and DEMA countermeasures are essential to protect devices that use cryptographic keys, especially sensitive defense applications that require strong anti-tamper protection of advanced electronics and commercial devices that perform high-value processing, including mobile devices and Internet of Things (IoT) endpoints.

A U.S. Department of Commerce report found IP theft costs U.S. companies $200 billion to $250 billion annually, while the Organization for Economic Cooperation and Development (OECD) estimates counterfeiting and piracy cost companies as much as $638 billion per year. The SmartFusion2 and IGLOO2 FPGA's design security protocols protect confidentiality, integrity and authenticity of the customer's design IP throughout the life cycle of the FPGA, substantially reducing the risk of IP theft during manufacturing or from fielded systems. Complementing the FPGA's built-in features such as a hard true random bit generator, the Athena TeraFire IP allows users to build tamper-resistant systems using secure Microsemi FPGAs that further use the Athena soft IP and cryptographic techniques to prevent system-level counterfeiting, and to provide other information assurance services vital to the security of the user's system.

This integrated security solution of Microsemi FPGAs with the TeraFire DPA-resistant cryptographic cores, with its combination of advanced security and countermeasures, provides a safe, tamper-resistant environment for use of cryptographic keys. This is accomplished by limiting information leakage in both power consumption—protecting against DPA, simple power analysis (SPA) and correlation power analysis (CPA)—and electromagnetic emissions—protecting against simple electromagnetic analysis (SEMA) and differential electromagnetic analysis (DEMA).

Microsemi has been granted certification of all SmartFusion2 and IGLOO2 FPGAs for seven protocols and services used to implement design security in these devices under the DPA Countermeasure Validation Program developed by Rambus Cryptography Research Division after a thorough assessment by an accredited third-party security laboratory.

Integrated into an easy-to-use security solution, customers can now embed strong IP and data protection into a wide variety of applications, including anti-tamper and information assurance, as well as wired and wireless communications. For more information on Microsemi's FPGA and SoC security capabilities, visit http://www.microsemi.com/products/fpga-soc/security#overview.

Availability

Microsemi's SmartFusion2 SoC FPGAs and IGLOO2 FPGAs are available to existing and new customers

now. For more information, email Sales.Support@Microsemi.com.

About Microsemi's Defense and Security Product Portfolio
Microsemi is a provider of defense and security products and services, including secure FPGAs and SoCs, secure solid state drives (SSDs), security software, anti-tamper solutions, FIPS-197 certified 1 Gigabit Ethernet and 10 Gigabit Ethernet PHYs with AES-256 MACsec support (IEEE 802.1AEbw-2013). Microsemi security services include risk assessment, protection planning, red teaming, blue teaming, security engineering and side channel analysis and mitigation. For more information about Microsemi's portfolio for defense applications, visit http://www.microsemi.com/applications/defense. For more information on Microsemi's security capabilities, visit http://www.microsemi.com/applications/security.

About Microsemi
Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,600 employees globally. Learn more at www.microsemi.com.

About The Athena Group, Inc.
Athena is a leading provider of security, cryptography, anti-tamper, and signal processing IP cores to many of the world's largest semiconductor companies, defense contractors, and OEMs, as well as emerging providers. Embedded in millions of ASIC and FPGA devices, Athena technologies enable high-value solutions where security and performance are mission critical – defense and aerospace, vehicle safety (V2V, V2X, telematics), networking and communications, satellites, cellular base stations, handsets, the Internet of Things (IoT), and more.

Athena's innovative and experienced team architects best-in-class products: security microprocessors with unmatched hardware efficiency and programmable flexibility, dedicated accelerators for cryptography and security protocols, a comprehensive set of tamper-resistant security cores with SCA/DPA countermeasures developed under a Developer agreement with Rambus' Cryptography Research division, highly optimized FFTs and signal processing cores for communications applications, and related technologies. For more information, visit athena-group.com.

# # #

"Safe Harbor" Statement under the Private Securities Litigation Reform Act of 1995: Any statements set forth in this news release that are not entirely historical and factual in nature, including without

limitation, statements related to its comprehensive portfolio of IP cores with SCA countermeasures based on advanced DPA countermeasure approaches with The Athena Group, Inc., are forward-looking statements. These forward-looking statements are based on our current expectations and are inherently subject to risks and uncertainties that could cause actual results to differ materially from those expressed in the forward-looking statements. The potential risks and uncertainties include, but are not limited to, such factors as rapidly changing technology and product obsolescence, potential cost increases, variations in customer order preferences, weakness or competitive pricing environment of the marketplace, uncertain demand for and acceptance of the company's products, adverse circumstances in any of our end markets, results of in-process or planned development or marketing and promotional campaigns, difficulties foreseeing future demand, potential non-realization of expected orders or non-realization of backlog, product returns, product liability, and other potential unexpected business and economic conditions or adverse changes in current or expected industry conditions, difficulties and costs of protecting patents and other proprietary rights, inventory obsolescence and difficulties regarding customer qualification of products. In addition to these factors and any other factors mentioned elsewhere in this news release, the reader should refer as well to the factors, uncertainties or risks identified in the company's most recent Form 10-K and all subsequent Form 10-Q reports filed by Microsemi with the SEC. Additional risk factors may be identified from time to time in Microsemi's future filings. The forward-looking statements included in this release speak only as of the date hereof, and Microsemi does not undertake any obligation to update these forward-looking statements to reflect subsequent events or circumstances.

Source: Microsemi Corporation