CURTISS-WRIGHT

NEWS RELEASE

Curtiss-Wright FSM-2 2TB Removable Storage Module Undergoing FIPS 140-2 Encryption Certification for Protection of Critical Data-At-Rest

Rugged 3U SATA module currently under evaluation by NIST for AES-256-bit encryption

ASHBURN, Va. – January 8, 2017 – Curtiss-Wright's Defense Solutions division today announced that it has begun the process of certifying its rugged, removable 2TB Flash Storage Module 2 (FSM-2) to achieve Level 2 FIPS 140-2 validation for the AES-256 encryptors designed to protect sensitive data-at-rest. The module is currently under evaluation by the National Institute of Standards and Technology (NIST). The size, weight, power and cost (SWaP-C) optimized module enables the secure transport of sensitive data between a base station and deployed airborne, ground or naval platform. The FSM-2 provides direct-attached SATA storage independent of software driver, operating system, or processor type. The compact 1.0" pitch 3U module features industrial temperature MLC NAND Flash and is designed to meet the demands of the most rugged, deployed applications. The module can be easily embedded into mission computers, sensor processors, mission recorders, instrumentation recorders, and network file servers such as Curtiss-Wright's Compact Network Storage 2-Slot with Fibre Channel (CNS2-FC). Use of the FSM-2 can lower schedule and technical risk for deployed storage applications, providing a COTS storage solution that meets the rigorous scrutiny of FIPS 140-2 certification. Validation is expected to be completed in the second half of 2018.

"We are committed to delivering industry leading COTS-based solutions for protecting sensitive mission data," said Lynn Bamford, Senior Vice President and General Manager, Defense Solutions division. "Our customers are seeking cost-effective solutions for securing high density data pre- and post-mission. Achieving FIPS 140-2 certification for our 2TB FSM-2 module, as we did successfully for our 1TB FSM storage module, will ease the integration of trusted computing hardware into deployed platforms."

About FIPS 140-2 Encryption on the FSM-2 Module
The FSM-2 is undergoing validation by NIST for FIPS 140-2 Level 2 encryption. The AES256-bit encryption used on the module can be seeded by keys that are either internally generated via a FIPS-compliant random number generator (RNG), or externally supplied by the user. By design, there is no mechanism for accessing the internally generated key. The chosen mode of key management – internally generated

or externally supplied – is determined by the integrator's requirements and operational constraints. This flexibility allows system designers to respond to changing program security requirements. Both internally-generated and externally-provided keys can be saved in two types of non-volatile memory or can be 'not saved' in volatile memory. Some applications require the keys to be automatically deleted upon every power loss as a security measure (e.g. more secure transport). In those applications, volatile memory storage is the proper choice.

Externally-provided keys can be restored to volatile memory, unlike the internally generated keys. To secure data by sanitization, a zeroize signal is accepted by the FSM. The zeroize signal is generated either by a software command, by pressing the push button on the FSM-2's front panel, or via a discrete input. After the keys are zeroized (deleted), the data cannot be accessed. In addition to a front panel LED indicator, key status is also provided via a user control interface. The non-volatile SRAM is a special non-imprinting type while the non-volatile EPROM is cleared with a special algorithm. As part of FIPS Level 3 requirements, anti-tamper on the FSM-2 involves placement of special seals that would be visibly damaged if the module were opened. Additional anti-tamper features are built into the FSM-2 electronics.

Sales inquiries: Please forward all Sales and reader service inquiries to ds@curtisswright.com.

For more information about Curtiss-Wright's Defense Solutions division, please visit www.curtisswrightds.com.

About Curtiss-Wright Corporation
Curtiss-Wright Corporation is a global innovative company that delivers highly engineered, critical function products and services to the commercial, industrial, defense and energy markets. Building on the heritage of Glenn Curtiss and the Wright brothers, Curtiss-Wright has a long tradition of providing reliable solutions through trusted customer relationships. The company employs approximately 8,000 people worldwide. For more information, visit www.curtisswright.com.

###

Note: Trademarks are property of their respective owners.