EWA - Canada

EWA-C File 1439-010

27 August 2007

Digital Security Controls, a Division of Tyco Safety Products Canada Ltd.
3301 Langstaff Road
Concord, ON L4K 4L2
Canada

Attention: Dan Nita, Approvals Manager

Reference: Quote EWA-C 070524-036A

Dear Dan Nita:

Subject: Advanced Encryption Standard Algorithm Validation Certificate No. 606

The following algorithm validation certificate has been issued by NIST and CSE for the SG-SYSTEM IV, Version 1.00 (Firmware). Please find enclosed:

For SG-SYSTEM IV, Version 1.00:

- Advanced Encryption Standard Algorithm Validation Certificate, Certificate No. 606.

Congratulations on your AES algorithm implementation validation!

Yours truly,

ELECTRONIC WARFARE ASSOCIATES-CANADA, LTD.

Carol Cantlon
Project Manager FIPS 140-2 Validations

Encl: 1

55 Metcalfe Street, Suite 1600
Ottawa, Ontario K1P 6L5
www.ewa-canada.com

Tel. (613) 230-6067
Fax (613) 230-4933
E-mail: ewainfo@ewa-canada.com

Advanced Encryption Standard Algorithm Validation Certificate

Certificate No. 606

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

The National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) hereby validate the Advanced Encryption Standard (AES) algorithm testing results of the implementation identified as:

SG-SYSTEM IV, Version 1.00 (Firmware)

and supplied by:

Digital Security Controls, a Division of Tyco Safety Products Canada Ltd.

in accordance with the specifications of the *Advanced Encryption Standard (AES)* (FIPS 197) and *Recommendations for Block Cipher Modes of Operation* (SP800-38A 2001 ED) as indicated on the reverse of this certificate. Implementations bearing the same identification and manufactured to the same specifications as the validated implementation may be labeled as complying with FIPS 197 for the modes, states, and key sizes identified in this certificate. No reliability test has been performed and no warranty of the implementation is either expressed or implied.

The validated implementation was tested using the following operating environment (for software implementations, operating environment includes processor and operating system; for firmware implementations, operating environment includes processor only; for hardware implementations, operating environment is not applicable):

Freescale MPC885

The vendor should be contacted to obtain a list of operating environments that support the validated implementation. Likewise, the vendor should be contacted to obtain a list of products/applications that use the validated implementation.

This certificate must include the following page that details the scope of conformance and includes the validation authorities' signatures.

The NIST document, *"The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)"* describes a series of known answer, multi-block message and Monte Carlo tests for implementations of FIPS 197: *Advanced Encryption Standard*, using modes of operation specified in NIST Special Publication 800-38A 2001 ED, *Recommendation for Block Cipher Modes of Operation*. The scope of conformance achieved by the algorithm implementation identified as:

SG-SYSTEM IV, Version 1.00 (Firmware)

and tested by the accredited Cryptographic Module Testing laboratory: **EWA-Canada LTD, IT Security Evaluation Facility**
NVLAP Lab Code 200556-0
CAVS Version 5.3

is as follows. The validated implementation performs AES in the following modes of operation, states, and key sizes:

Mode(s) of Operation	State(s)	Key Size(s)
Electronic Codebook (ECB)	**Encrypt/Decrypt**	**128**

Signed on behalf of the Government of the United States

Signature: William C Barker

Date: July 23, 2007

Chief, Computer Security Division
National Institute of Standards and Technology

Rev. 04/2006

Signed on behalf of the Government of Canada

Signature:

Date: 13 August 2007

Director, Industry Program Group
Communications Security Establishment