Information Assurance and Consultancy Services

A2h, Hubble Road,
Cheltenham, Gloucestershire, GL51 0EX

Tel: 01242 221491 Ext 30074
Fax: 01242 709194
GTN: 1366 Ext: 30074
E-mail: iacs@cesg.gsi.gov.uk

CESG Ref: X/32984/4204/02
28 October 2008

CESG SECURE SANITISATION APPROVAL

Company:	**Blancco Ltd**
Product:	**Blancco 4.8 HMG Software**
Version:	**Version 4.8 HMG**
Erasure Test Platform:	Dell Precision 410 workstation
Erasure Standards:	**Lower Level & Higher Level Overwriting [IS5]**
CESG Reference:	**SS014**

References:

[IS5]	HMG Infosec Standard No. 5, Secure Sanitisation of Protectively Marked or Sensitive Information, Issue 2.0, September 2007.
[ManS]	CESG Information Assurance Manual S: Guidance on Secure Sanitisation & Disposal, Issue 2.0, September 2007.
[Rep]	QinetiQ Test Report: Assessment of Disk Wiping Product, Blancco – HMG Software v4.8, QINETIQ/AT/DS/TR0800357, Issue 2.0, 24/10/08.
[UG]	Blancco 4.8 HMG Software Manual, Version 4.8 HMG.

The secure sanitisation product described above has been assessed by the QinetiQ Data Recovery and Computer Forensics Laboratory (DRFL) Service and has been checked for compliance against the requirements of [IS5] and [ManS].

The QinetiQ DRFL has concluded that, when installed, configured and operated correctly, as described in the User Guide [UG] and overleaf, this product is suitable for wiping disks to the [IS5] standards at the Lower Level and Higher Level Overwriting Standards, in accordance with [ManS].

CESG – the National Technical Security Authority for Information Assurance – has completed their examination of the QinetiQ DRFL Test Report and has therefore determined that this product meets the [IS5] erasure standards for secure sanitisation in accordance with [ManS], subject to the operational and risk management aspects noted overleaf.

Jeff Stanford
Head of CESG Assurance Services

STATEMENT OF SECURE SANITISATION FUNCTIONALITY

PRODUCT NAME – Blancco 4.8 HMG Software

1. Secure Sanitisation Functionality

Blancco 4.8 HMG Software provides the capability to meet the erasure standards listed below for a range of media and platforms as specified in the User Guide [UG] delivered with this product. The specific range of Maxtor, Quantum, Samsung, Seagate, and Western Digital hard disk drives that have been tested are detailed in the QinetiQ Test Report [Rep]. The 11 drives tested included interface types of IDE (7), SCSI (3) and SATA (1).

The tests were performed on a Dell Precision 410 workstation, using Blancco 4.8 HMG Software and the User Guide [UG].

2. Erasure Standards

When used correctly, as summarised below, Blancco 4.8 HMG Software is designed to be approved for the Lower Level and Higher Level Overwriting Standards in accordance with [IS5] and [ManS] for the above media types that are storing data at Impact Levels IL0 to IL6 inclusive.

3. Operational Aspects

Blancco 4.8 HMG Software must be securely delivered, installed, configured and operated in accordance with [UG], [IS5], [ManS] and the purchaser's own Security Operating Procedures, together with the guidance provided in the QinetiQ Test Report [Rep].

Blancco 4.8 HMG Software should be included in the periodic review for security updates to security products included in the purchaser's system.

4. Risk Management Aspects

Prospective purchasers should note that the Approval only extends to the media and platform types tested. Although testing of all types is not possible, due to the extensive range available, the testing performed provides some degree of assurance that the erasure functionality should operate similarly on the other media and platform types detailed in [UG].

Any patches to Blancco 4.8 HMG Software and the operating system should be reviewed for their impact on product security and should be applied in accordance with the host system's risk management policy/plan.

Note that the procedures for the secure sanitisation and disposal of magnetic, semiconductor and optical computer storage media are set out in [ManS]. It should be read in conjunction with [IS5], which gives advice on managing the security risks that arise when computer storage media holding protectively marked or sensitive information is released into less secure or insecure environments.