Australian Government

Department of Defence
Intelligence, Security and International Policy

DSD'S CONSUMER GUIDE

BAE SYSTEMS AUSTRALIA INTERACTIVE LINK MULTIPLE COMPUTER SWITCH WITH USB INTERFACES (MCS ULTRA V1.1)

Product Description

The BAE Systems Australia (BAE) Interactive Link Multiple Computer Switch with USB Interfaces (MCS Ultra) is a keyboard/video/mouse (KVM) switch designed to allow for two computers on different networks to share a single USB keyboard, VGA monitor and USB mouse. The user selects the computer they wish to use by pressing one of two (2) buttons on the front of the device. Visual indication of the selected computer is provided above the buttons and an audible buzz activates when switching between computers, providing a multi-sensory indication of a change in domain.

Evaluation Scope and Summary

The scope of the evaluation included all functionality of the BAE MCS Ultra switch, in particular its ability to maintain separation of information even under failure conditions. The model evaluated was the FID005 version 1.1.

The product has been evaluated to meet the requirements of a High Grade (HG) product and has been given a High Grade Assurance Level.

DSD Findings

The BAE MCS Ultra switch can be used between any two systems of the following classifications.

- UNCLASSIFIED
- X-IN-CONFIDENCE
- RESTRICTED
- PROTECTED
- HIGHLY PROTECTED
- CONFIDENTIAL
- SECRET
- TOP SECRET

Usage Caveats

For Australian Government users, the following conditions need to be adhered to use the device at a High Grade level of assurance.

- Australian Government users are recommended not to connect a KVM switch to another KVM switch.
- Australian Government users are recommended not to use wireless peripherals or wireless capabilities in any of the computers.
- The KVM must be housed in a facility accredited to process data to the level of the highest classified system connected to the KVM. For example, if a system classified TOP SECRET is connected to the KVM, the surrounding facility must be accredited to be able to process TOP SECRET data.

Additional information on the selection of KVM switches can be found in the Information Security Manual (ISM), also known as ACSI 33, under the "Peripheral Switches" heading

DSD's Recommendations

In addition to the usage caveats, DSD makes the following recommendations for Australian Government users.

When setting up the MCS Ultra

- Use different passwords for each system connected to the MCS Ultra.
- Provide a visual indication on the monitor for each system, particularly identifying the classification.
- Clearly identify the system that each of MCS Ultra buttons corresponds to.
- Install the device in a trusted environment.
- Check there are no signs of blistering or peeling on the tamper seal and that it is intact before using the MCS Ultra.

When using the MCS Ultra

- Periodically, check that the tamper seal for damage.
- Lock screens or log out before switching domains.
- Stop typing before switching domains.
- If keystrokes or mouse movement are not reflected in the monitor, treat as a data spill according to the ISM.
- Do not use the MCS Ultra in a high TEMPEST threat area.

Australian Government users are advised that the reset button and ready indicator on the front of the device do not serve any function.

Repairs and Disposals

The MCS Ultra must be returned for repairs if:

- the unit switches to the wrong domain;
- the current domain does not correspond to the indicating LED light;
- the LED lights do not function or the buzzer does not sound when changing domains;
- the display seems unusual, including flickering, fuzziness, mixed video signals from both computers, and unexpected colours; and/or

- there is any unusual behaviour (such as switching without pressing any button).

Before returning the device to the manufacturer for repairs, it must be sanitised in accordance with the ISM section titled “Product Sanitisation and Disposal”. Also refer to this section for policy on disposing of the unit.

Point of Contact

For further information regarding the certification of these products or compliance with the ISM, please contact DSD on (02) 6265 0197 or email assist@dsd.gov.au.

ACSI 33

The advice given in this document is in accordance with ISM release date September 2008. Australian Government agencies are reminded to check the latest release of ACSI 33 at www.dsd.gov.au/library/infosec/acsi33.html.

Date of this Consumer Guide

This Consumer Guide was issued by DSD on 27 October 2008.