DATA SECURITY WITHIN GOVERNMENT AGENCIES THROUGH SECURE KVM MATRIX SWITCHES

OVERVIEW

Certifications and Compliance

- **NIAP Certified** - Peace of mind knowing it is NIAP Common Criteria Protection Profile (PP) for Peripheral Sharing Switch (PSS) v.3.0 compliant.
- **Protection Profile** - The NIAP Version 3.0 Protection Profile for Peripheral Sharing Switches defines the requirements for use of Secure Desktop KVM Switches. Compliance with Protection Profile for Peripheral Sharing Switches Version 3.0 ensures peripheral sharing capabilities provide maximum user data security when switching, preventing unauthorized data flows or leakage between connected sources
- **Common Criteria (CC) Certification** - Evaluates KVM (Keyboard-Video-Mouse) switches, KM (Keyboard-Mouse) switches, KVM splitters (Reverse KVMs), and (not covered in PP 3.0) using the Protection Profile for Peripheral Sharing Switches.
- **TAA/BAA Compliant** - Our secure switches are TAA/BAA compliant and provided by Vertiv, an American company.

Problem

Internal Security Threats

Government agencies require secure access to information that often has differing levels of classification. This may require viewing classified information on one monitor and information from a different classification level on a separate screen. Users are often required to securely integrate information from several isolated sources on multiple displays in real-time.

These agencies are increasingly reliant on electronic systems and require the use of internal communications networks in addition to the Internet. They not only need to protect themselves from external cyber threats, but also threats internally. Within these various government agencies, data is at risk of being compromised by insiders via their desktop, thin client, or laptop computers.

Because of this, there is a real need for greater privacy and security when it comes to accessing data. Specific networks provide additional levels of privacy and classified security. Examples of these networks include NIPRnet (private IP network), SIPRnet (classified), and JWICS (highly classified), etc. For a user, multiple computers (dedicated to SIPRnet or JWICS, for example) are connected to a Secure KVM switch. This is common throughout the Department of Defense and in the Intelligence Community. Peripherals such as a keyboard or mouse are capable of both sending and receiving data that is not secured, therefore leaving a security gap.

Solution

Addressing these threats with Secure KVM Switches

A secure KVM desktop matrix switch is very similar in features and capabilities to a standard secure KVM switch, but takes both security and ease of use to the next level. With the Cybex secure desktop matrix, users are able to concurrently view two computers across various security domains and switch back and forth. Through **Cursor Navigation Switching (CNS)**, a user is not required to push a button to select the computer that they are working from, but can move back and forth easily between the two displayed sessions. One mouse and one keyboard will move the user from one computer to the other.

The Vertiv™ Cybex™ SCM100 series of secure desktop matrix KVM switches offers a proven solution for guarding against cyber intrusion at the desktop. They also provide users with high resolution compatibility utilizing HDMI, DisplayPort and traditional DVI technology.

DATA SECURITY WITHIN GOVERNMENT AGENCIES THROUGH SECURE KVM MATRIX SWITCHES

The Cybex SCM 100 secure desktop Matrix KVM switch offers a proven solution for guarding against cyber intrusion at the desktop.

- Independently switched display connections - situational awareness of any two connected systems.
- Hardware-based peripheral isolation loads all firmware on ROM with no keyboard buffering or memory.
- Dedicated Peripheral Port permits a secure connection to approved external USB devices, including CAC smart card readers, fingerprint readers, and face recognition devices.

Other requirements of the secure KVM matrix include:

EDID Emulators - Extended Display Identification Data.

DPP - Dedicated Peripheral Port for secure connection to USB peripherals including two-factor authentication devices such as CAC smart card readers, fingerprint readers and facial recognition.

Active Tamper Detection - Active Tamper Detection causes the KVM system to become inoperable if the housing has been opened.

Locked Firmware - Locked Firmware prevents any attempts to alter the operation of the KVM.

Push-Button Control - Push-Button Control requires physical access to KVM when switching between connected computers.

VertivCo.com | **Vertiv Headquarters,** 1050 Dearborn Dr. Columbus, OH 43085, USA

AV-49521 (R04/19)