DATA SECURITY WITHIN GOVERNMENT AGENCIES THROUGH SECURE KVM 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** - Common Criteria evaluates KVM (Keyboard-Video-Mouse) switches, KM (Keyboard-Mouse) switches, KVM splitters (Reverse KVMs), and Multi-viewers 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

Many government agencies are increasingly reliant on electronic systems and require the use of internal communications networks in addition to the Internet. These agencies 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 or laptop computers. These “internal” attacks need to be addressed in the same manner as any attack originating outside the organization.

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).

With a standard (or traditional) KVM, all of the information from the keyboard, mouse, monitor, etc. occurs in one switching location inside of the KVM switch. As such, a standard (or traditional) KVM switch is a potential cyber risk enabling unauthorized access to multiple networks. With this in mind, organizations need secure solutions that meet stringent government security standards to protect data from both internal and external cyber threats.

Solution

Addressing these threats with Secure KVM Switches

For a user, multiple computers (dedicated to SIPRnet or JWICS, for example) are accessed via a Secure KVM switch. This is common throughout the Department of Defense and in the Intelligence Community.

A secure KVM switch allows authorized users to switch between networks with various security levels from a single position. With a secure KVM switch, each port is isolated from the others to prohibit data from being transferred between connected computers. This is accomplished through Unidirectional Optical Data Diodes (UODD), which limits data to moving in one direction only. When information passes through the Secure KVM Switch, it is limited to where the data can be sent. Additionally, to prevent eavesdropping, the buffer is automatically cleared after any transmission of data.

DATA SECURITY WITHIN GOVERNMENT AGENCIES THROUGH SECURE KVM SWITCHES

Other requirements of a secure KVM include:

- **EDID Emulators** - Extended Display Identification Data.
- **DPP** - Dedicated Peripheral Port for secure connection to approved 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 seals have been penetrated.
- **Locked Firmware** - Locked Firmware prevents attempts to alter the operation of the KVM.
- **Push-Button Control** - Push-Button Control providing physical access to KVM when switching between connected computers.

If you must guard against cyber intrusion or must access data at multiple classifications, Vertiv™ Cybex™ secure KVM switches provide the protected access needed to for peripheral sharing devices.

The Vertiv Cybex™ SC800/900 secure desktop KVM switching portfolio offers a proven solution for guarding against cyber intrusion at the desktop. These switches are designed specifically to the stringent specifications of the U.S. government and comply with the requirements of the NIAP Protection Profile for Peripheral Sharing Switches Version 3.0. These switches provide users with high resolution compatibility utilizing HDMI and DisplayPort technology, as well as, traditional DVI technology.

These products allows users to switch safely and securely between computers operating at different security classification levels from a single set of peripherals, providing continuous access to critical data. Employing multiple security features, the secure design prevents the transfer of data or information between the connected computers, ensuring data security is not compromised.

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

AV-49522 (R04/19)