VERTIV WHITE PAPER

How Government Agencies Deliver the Mission

Enabling Secure, Rapid Access to Classified Information

Ensuring Security, Speed and Productivity with Mission-Critical Operations

Mission-critical personnel power critical operations for myriad government agencies. They're found analyzing vast amounts of confidential data, delivering vital agency services, running command and control centers, directing military and national security missions and overseeing information security and business continuity programs, among other responsibilities.

This work is complex, collaborative and often highly confidential. As a consequence, staff must abide by information and access controls and information handling restrictions. Top-secret and sensitive compartmented information (SCI) is routed over internal networks including the Joint Worldwide Intelligence Communications System (JWICS). Secret information is routed over internal networks including the Secret Internet Protocol Router Network (SIPRNet). And finally, unclassified information is routed over the Non-Classified Internet Protocol Router Network (NIPRNet).

In addition, staff must synthesize vast amounts of information and work collaboratively with teams in an environment where accurate decision making is critical and every minute counts. While industry companies operate by the principle of least privilege granted to provide access to systems, applications and data, government agencies have much more restrictive access control policies personnel must abide by. As a consequence, standard keyboard, video and mouse (KVM) switches, which enable users to access different systems and screens on one monitor, aren't sufficient for classified government work. These agencies need a different type of solution that meets their heightened mission and security requirements: enabling authorized users to access multiple compute resources with varying security classifications on a single screen and use robust features to perform their work. That solution is a secure multiviewer KVM.

Secure Multiviewer KVMs Enable Mission-Driven Work

Secure multiviewer KVMs can be used either to access multiple compute resources on a single workstation or project them on a video wall in secure environments, such as command centers.

Government Agencies Need Secure Multiviewer KVMs for Mission-Critical Operations

Government agencies are seeking to accomplish multiple objectives as they empower authorized workforces to use their compute resources. These objectives include:

Ensuring Data Integrity – In addition to maintaining access controls, secure multiviewer KVM solutions must provide ultra-secure data handling, preventing such actions as copying, cutting and pasting of information across classification levels. This prevents cross-contamination and preserves data integrity and security.

Enabling Multi-Screen Viewing – Staff, such as analysts, military staff and information security teams, digest torrents of data. The ability to view multiple compute resources on a single screen and switch securely among them is critical to enabling key business operations.

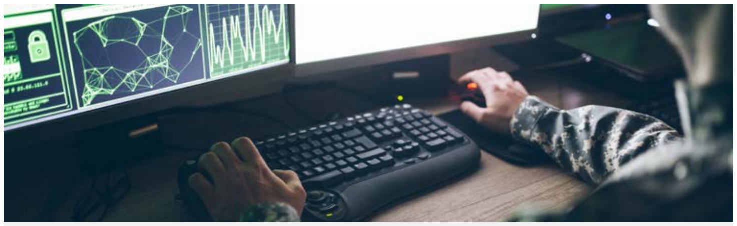
Facilitating Fast and Seamless Switching – Much like other fast-paced, digitally driven industries, government agency personnel make decisions in real-time. Secure multiviewer KVM solutions enable users to access, view and switch among compute resources without latency, which could harm the mission and degrade team and individual performance.

Driving User Productivity – Secure multiviewer KVMs reduce the friction of work processes, with intuitive and rich features that support daily work, such as touching screens to interact with applications and using cursors to guide switching. They enable users to scale, window, tile, cascade and consolidate compute resources, boosting their speed and productivity, while also providing an ergonomic-friendly work environment.

Rightsizing Compute Resources to Real Needs – The federal sector is a major IT buyer, accounting for nearly $92 billion in spending in 2020. Like other industries, government agency decision makers would rather spend resources on innovation than infrastructure. Secure multiviewer KVM solutions enable personnel to achieve persistent awareness of multiple computers with different security classifications and limit the number of keyboards and mice to just one per user. As a result, government agencies can reduce spending on cables, keyboards and mice, freeing up funds for new initiatives without impacting operations.

Saving Space – Multiple compute resources clutter desks and work environments. Secure multiviewer KVMs enable government agencies to save on space, potentially adding more staff in a single work environment or operating efficiently in space-constrained environments, such as military airplanes and ships.

Key Federal Use Cases for Secure Multiviewer KVMs



Time-Sensitive Operations – Time-sensitive operations such as military missions require that analysts view and analyze multiple resources with different classification levels at speed. Productivity features such as windowing, tiling and easy cursor navigation switching enable real-time operations, while also preventing analyst fatigue due to unnecessary keystrokes. Analysts can also create custom views to save time.

Military Mission Planes and Ships – Like command centers, these environments are highly secure, but space may be constrained. Secure multiviewer KVMs can be used to enable access to computer resources that are typically fewer in number, such as four PCs at once, to power operations.

Command Centers – Government agencies operate command and control centers and secure rooms, where everyone shares the same clearance level. In these environments, the secure multiviewer KVM can be used to project up to 16 compute resources on to a video wall for all to see. One analyst can drive switching, enabling others on the team to view and synthesize information, collaborating rapidly on strategic decisions or next steps.

Briefing Rooms – Secure multi-viewer KVMs help facilitate secure briefings by providing access to all the information participants need. They provide inputs to video walls or large screens for senior leaders to analyze.

Conclusion

Information is growing in volume, variety and velocity, making mission-critical operations ever more complex. Government agencies seek to equip personnel and teams with digital solutions that enable secure access to information at various classification levels, enable collaboration and enhance productivity and work environments. The Vertiv™ Cybex™ Secure KVM MultiViewer can help government agencies accomplish all of these aims, improving their ability to deliver on their mission.

Vertiv is your partner in delivering the mission by protecting information and enabling authorized access to classified resources. To learn more visit https://www.vertiv.com/en-us/products-catalog/monitoring-control-and-management/secure-kvm/vertiv-cybex-secure-multiviewer-kvm-switch/

Introducing the Cybex™ Secure KVM MultiViewer

The Vertiv™ Cybex™ Secure KVM MultiViewer is designed for government agencies that operate in heightened security environments.

Solution benefits include the ability to:

- Simultaneously view up to 16 computers on a single monitor
- Interact with information at different classification levels on a single screen
- Enable seamless keyboard and mouse control switching with Cursor Navigation Switching (CNS)
- Reduce compute peripherals for personnel, decreasing IT costs and clutter
- Directly interact with any application using native touch screen capabilities
- Authenticate users across multiple secure computers using smart card (CAC) or biometric readers
- Increase flexibility, with either DisplayPort (DP) or HDMI direct connections
- Mix different computer display types, meeting agency mission needs

Arne Holst, "Federal government information technology (IT) expenditure in the United States from FY 2011 to FY 2021," Chart, Statista, April 3, 2020, https://www.statista.com/statistics/506409/united-states-federal-it-expenditure/

VERTIV™

Vertiv.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA