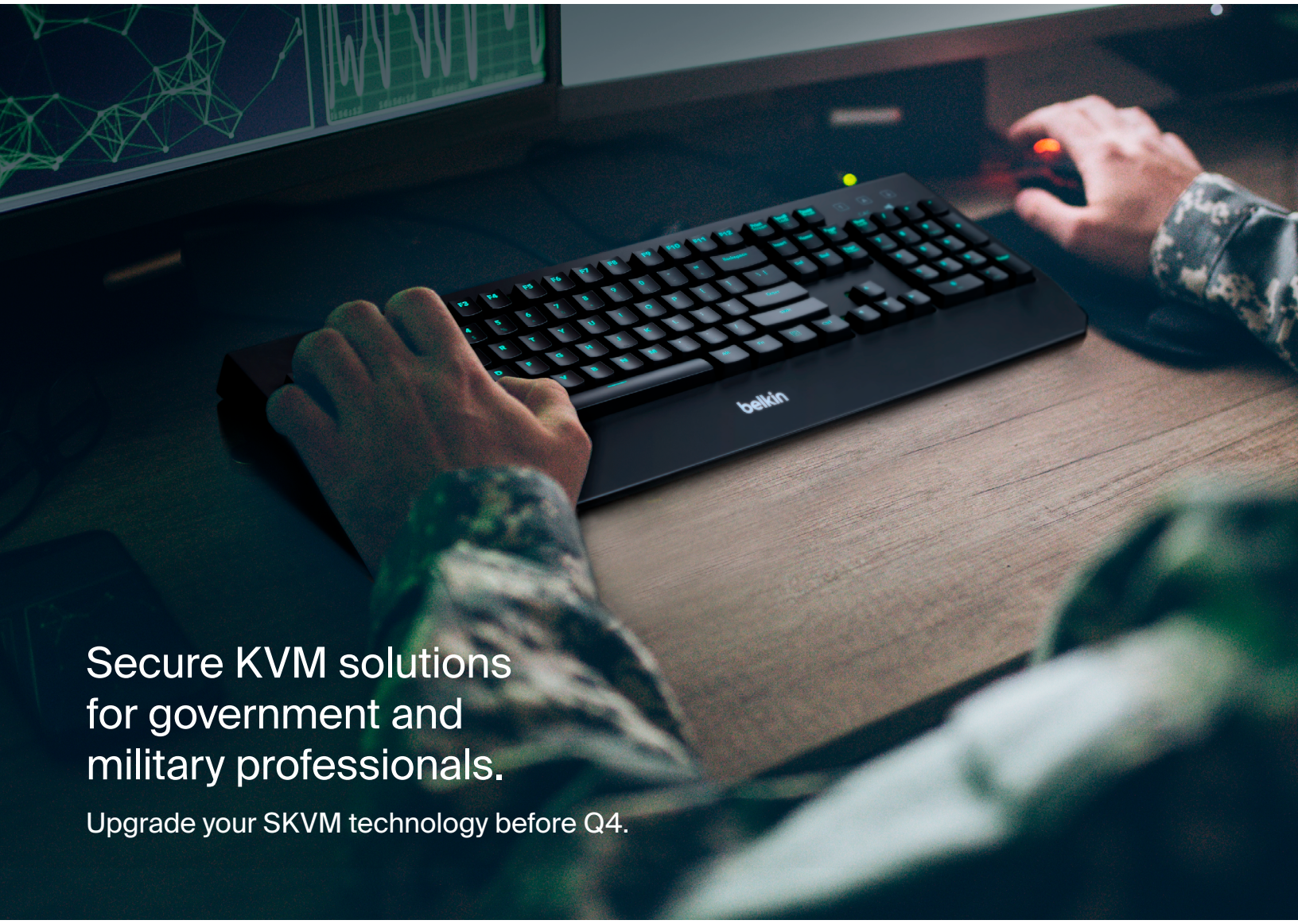

Secure KVM solutions for government and military professionals.

Upgrade your SKVM technology before Q4.

The Belkin Cybersecurity Dispatch newsletter covers Secure KVM news and solutions for government and military professionals. Belkin debuted Secure KVMs for government and military applications in 2006, and since then we've helped innovate products and move the needle on NIAP and Common Criteria standards.

We work with companies and agencies to safeguard valuable networks, centralize administration, and reduce infrastructure costs. Among Belkin first-to-market cybersecurity innovations are Secure KVMs, Secure KVM Remote with Integrated Keyboard, and Universal Video Compliant Secure KVMs.

During Q3, government and military agencies are in "use it or lose it" mode. Belkin is showcasing cybersecurity products that will help your business spend its allotment by September 30. It's the perfect time to update your technology with our Modular SKVMs and KVM Remote Control with Integrated Keyboard so you don't end up being a (budget) loser.

PP3.0 vs. PP4.0

The latest Common Criteria/NIAP standard, NIAP Protection Profile for Peripheral Sharing Devices version 4.0, offers myriad advantages over the previous NIAP PP PSS 3.0, established in 2015. Among these are improved security requirements and clearer-defined guidelines for allowed and prohibited devices. By upgrading to NIAP PP PSD 4.0, federal organizations can ensure their networks are secured against both sophisticated and basic hackers, which is critical as cyberattacks proliferate.

Security Function	PP PSS 3.0	PP PSD 4.0
Passive Anti-Tamper	Tamper labels	Tamper labels
Active Anti-Tamper	Battery backup mandatory	Active anti-tamper is optional
Audit Log	Mandatory	Optional unless active anti-tamper is implemented or programmable USB peripheral port is supported
Field firmware updates	Not allowed	Defined patches allowed with audit-log and only with authenticated admin account
Audio Input	Not allowed	Optional only if no other switching function claimed (i.e., no video, KM, authentication device). Data diode required if audio input supported.
Audio Output	Analog only, audio diode required for 40dB up to 20KHz isolation	Analog output or digital with video; 40dB isolation up to 60KHz; 8th-order elliptic filter required; isolation must be maintained in tamper mode or power off; ability to split audio from keyboard/ mouse controls.
Keyboard/Mouse	Optical data diode, PS/2; KM only mode	USB emulation for HID input; configurable ports for approved peripherals with ability to whitelist/blacklist specific devices; guard mode for KM switching; PS/2 support removed.
Video	VGA, DVI, HDMI, and DP	VGA, DVI, HDMI, DP, USB-C; DP to HDMI to DP conversion specified to physically block potential backchannel; ability to provide 2nd level video rendering for PiP and multiviewer capabilities.
General	Peripheral device filter (authentication device, KM, etc.)	Peripheral device filter and acceptance/rejection bi-color LED; remote controls; definitions for KVM extenders, isolators. Explicitly prohibits multi-user matrix.

KVM Remote Control with Integrated Keyboard

F1DN008KBD

The Belkin KVM Remote Control with Integrated Keyboard ushers in a new era of Secure KVM user experience. Pairing it with a Belkin Universal and Modular Secure KVM provides channel selection options for 1-8 port KVMs and mimics the color configuration of the front panel in the backlit USB keyboard. Combined with the mounting options available for Secure KVMs, it allows efficient enclave remote control and operator awareness, while providing an optimally decluttered workspace.

Use Cases

For companies and agencies that utilize color as an indication of the security enclave, the integrated keyboard provides a clear, visible indicator for operators as to which enclave they are working on.

Key features and benefits:

- Compatible with Universal 2nd Gen SKVMs – 2-, 4-, and 8-Port Models and Modular SKVM – 2-, 4-, and 8-Port Models
- Mechanical, high reliability keys
- Single USB connection
- Colorization configuration of KVM keys and overall keyboard
- User-configurable light intensity
- CAC and audio freeze indicators
- Easy to install and deploy – installation instructions included
- Rugged construction with black texture finish
- 6-foot Kevlar sheathed connection cable
- Operates with Belkin console extenders
- TAA-compliant
- Belkin 3-year warranty

Modular SKVM

F1DN208MOD-BA-4

The Belkin Modular Secure KVM series packs the latest in Common Criteria and NIAP Protection Profile version 4.0 design requirements in the smallest form factor available. An included remote control and innovative mount options allow administrators to craft operator stations to meet security requirements while decluttering the desk.

TAA-compliant, purpose-built cables help IT administrators circumvent compatibility issues during installation, maintenance, and upgrades. This flexibility enables IT managers to deploy the same Secure KVM switch across their network without needing expensive and unreliable video converters while extending the usable life of the Secure KVM.

Use Cases

The Belkin Secure KVM series is ideal for use in IT environments that demand rigorous cybersecurity provisions — including government, military, and healthcare applications. Ideal for highly sensitive applications that demand isolation between different network security enclaves, the Belkin Modular Secure KVM switches utilize optical data diodes and peripheral emulation on each channel. This helps prevent data leakage between computers while maintaining strict air-gap isolation, even when sharing peripherals.

Key features and benefits:

- Designed for NIAP PP PSD 4.0 compliance
- Video support for up to 4K (3840x2160), @30Hz refresh
- Optional DP, mDP, DPMST, HDMI, DVI, VGA, and USB-C cables - host and console
- Modular form factor for maximizing desk space
- Supports up to eight host computers
- Supports up to two displays for the user
- Included remote-control unit
- Secure packaging: Tamper-evident packaging ensures product is not tampered with during transport

Industry News

Content condensed from articles that originally appeared on MeriTalk at **meritalk.com/articles/**

Navy prepped to deploy 'Amelia' AI NESD feature.

The U.S. Navy is preparing to deploy a new AI-based feature called "Amelia" as part of the Navy Expeditionary Sea Drone (NESD) program. The program is designed to provide autonomous capabilities for the Navy, allowing it to collect and analyze data in real time, and respond quickly to changing circumstances.

The Amelia AI feature will be an integral part of the NESD program, providing advanced computing power and machine learning capabilities that will enable the drone to autonomously detect objects and respond accordingly. This will be a major step forward for the Navy, as it will allow them to use drones more efficiently in their operations while also reducing risks associated with manual operation of these vehicles.

The deployment of Amelia marks an important milestone in the development of AI technology for military applications, as it signals a shift towards increased autonomy on naval vessels. With this capability, sailors can focus on more strategic tasks while leaving mundane ones, such as object detection and navigation, up to Amelia.

Air Force unified in efforts to push zero trust.

The Air Force is unifying its efforts to push for a zero-trust security framework, which will help ensure the safety of their networks and data. This approach will help protect against malicious actors who are looking to exploit vulnerabilities in the system. It also helps reduce the risk of insider threats, as it requires authentication and authorization for all users before they can access any resources.

Using a combination of technologies, such as artificial intelligence, machine learning, and analytics, helps the Air Force to identify potential threats quickly and accurately. With this unified effort, they hope to create a more secure environment that can better protect them from cyberattacks.

"With zero trust ... the hype is real," said U.S. Air Force Chief Information Officer (CIO) Lauren Knausenberger. "It's happening. We are going to spend billions of dollars on this, and we have done the work to make sure that it is going to stick," she said. "I have not been this excited about an effort in the DoD in a really long time."

U. S. military playing catch up on telehealth initiatives.

As the world of technology develops, it's becoming more and more important for the U.S. military to stay up to date on the latest developments in order to achieve its healthcare goals. Integrating vital technologies into existing systems is one way the U.S. military can ensure that it remains on the cutting edge of healthcare delivery and outcomes research. The military is using technology to improve healthcare delivery while addressing some of the challenges they face when integrating these technologies into their existing systems.

"We are behind on implementing telehealth across all the services and within DHA... we're trying really hard to play catch up and figure out what we're doing on that," said Seileen Mullen, principal deputy assistant secretary of Defense for Health Affairs (DHA).

The U.S. military is lagging behind other countries in terms of integrating cutting-edge technologies into its healthcare system. This is despite the fact that these technologies can help improve patient care, reduce costs, and provide better access to medical services for service members and their families.

For questions, contact us at 800-282-2355 or federalbusinessdivision@belkin.com.

In the meantime, learn more about our products at belkin.com/cybersecurity