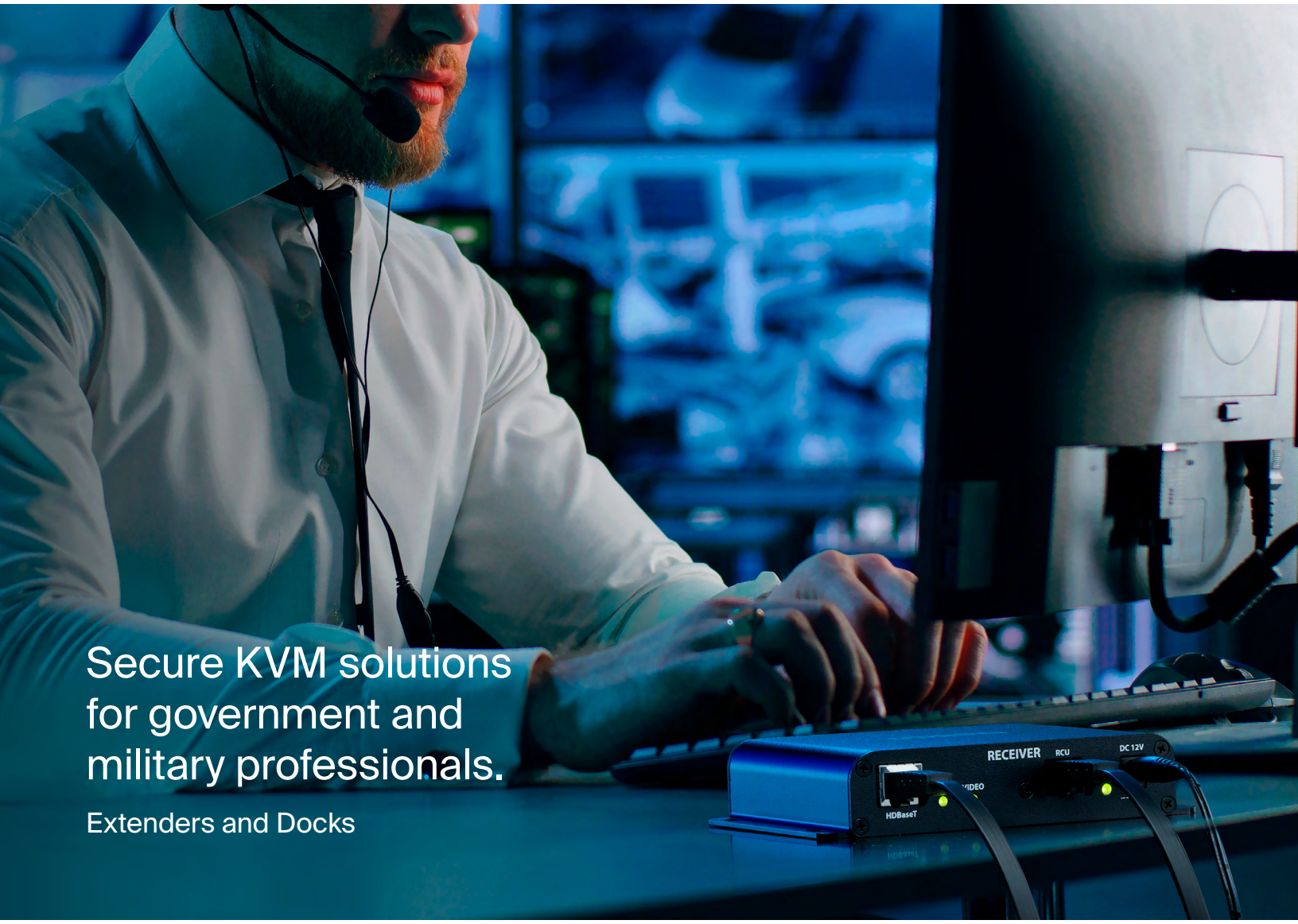

Secure KVM solutions for government and military professionals.

Extenders and Docks

Welcome to Q2's edition of the Belkin Cybersecurity Dispatch newsletter covering 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.

Belkin SKVM switches are purpose-built for mission-critical applications to positively impact and improve worker efficiency. As an industry leader, we're committed to creating solutions to connect and protect users working across multiple security enclaves.

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.

We are happy to announce the launch of our new products, Extenders and TAA Dock Solution. Continue reading to learn more about how these products improve security and productivity.

New Product Highlight

Belkin Extenders

Use Cases

Existing technology allows extenders to deliver point-to-point video and USB across distances, but users are unable to change security enclaves on an SKVM. Belkin SKVM keyboards and remote-control pads deliver groundbreaking technology by enabling enclave switching control over long distances from the user's desktop or lectern. This valuable security feature allows the processing side and the SKVMs to be located in a secure data center rather than at the desktop or conference. Leveraging its SKVM expertise, our extender solution is better than a zero or thin client — it's a no-client.

Key features and benefits:

- Improve security and centralize administration
- Dramatically reduce infrastructure costs
- Control computer, secure enclave or SKVM switch From up to 328 ft. with CAT6 or 984 ft. with SFP Fiber
- Designed for use on government and military networks with a Secure KVM
- Assembled in the USA, secure packaging ensures integrity from factory to user site
- US-based technical support
- TAA compliant

Belkin TAA Dock Solutions

Use Cases

Docks typically add more ports for users to work with, but this can adversely affect security. Belkin TAA-compliant docking stations offer built-in cables and less ports, increasing security while maintaining compatibility. Our purpose-built docks create a secure, expanded workspace that allows users to connect a mouse, keyboard, and video, while reducing desktop clutter with a single cable connection to the USB-C® laptop.

Key features and benefits:

- Provides greater security by eliminating unnecessary docking ports
- Reduces clutter through form factor and capabilities
- Improves deployment and user experience by eliminating quality and performance issues from non-Belkin or aftermarket docks
- Optimizes user experience by adding features
- Decreases SKUs required in solution, as an all-in-one dock with integrated cables
- Reduces total cost of ownership through features
- TAA compliant

Industry News

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

Army Deploys AI to Train Workers

AI technologies are being pressed into service by the U.S. Army to train workers and create predictive AI models. Senior leader and senior advisor of the U.S. Army's Office of Business Transformation, Bakari Dale, launched his Digital Transformation Summit keynote address with a speech prepared by the ChatGPT chatbot.

The speech capably covered the Army's key digital transformation efforts, including bolstering cybersecurity and data analytics, but Dale noted that the chatbot's speech lacked context. "It shows you that speech that it prepared hit all the topics that it needed to, it provided a general framework, but what it was missing was the context from the individuals who are living that daily life," said Dale.

Noting that one of his jobs is to look at technology to determine how the Army can employ it to make our country more secure, he added that the Army is employing AI to improve its digital workforce. Among the programs implementing AI is the Deep Green challenge data science competition, utilizing AI and machine learning to train the Army masses to develop AI models to accomplish great things. Additionally, the tool H2O.ai employs deep learning to use computer vision and LiDAR technology for autonomous vehicles, and AI platform DataRobot trains its workforce on machine learning.

New Navy Tech Boss Cites Infrastructure, Comms, and Cyber Initiatives

Jane Overslaugh Rathbun, named the Navy's principal deputy CIO in January, recently discussed her agenda at an event organized by Billington Cybersecurity. On the modernization front, she said, "we have made great progress in improving our infrastructure, but the work is never done, and if we're smart, we will always be continuing to improve."

Pivoting in the innovate arena, Rathbun revealed that the Navy is looking at things like 5G and commercial SATCOM with non-geostationary low-Earth orbit capabilities that can help meet Department of Navy mission needs. According to Rathbun, "these types of satellite communications could be a game changer for the Department of Navy with regard to access to bandwidth, afloat and ashore, in areas where we don't have this connectivity."

Being cyber ready and working with our DIB [(defense industrial base]) partners to help make them more protected is the priority in the defend space. "That's kind of where we will be headed," said Rathbun.

Marine Corps Unveils Software Factory Pilot

The U.S. Marine Corps' three-year pilot project Marine Corps Software Factory (MCSWF) intends to develop a Marine-led software development capability and evaluate demand and requirements for the factory effort's services. The project's goal will be to enhance the Corps' modernization efforts by empowering Marines to develop applications for commanders at the speed of relevance. Plans call for the MCSWF to leverage the Corps' recent talent management efforts, industry partnerships, and innovations in cloud technology.

Because the operating environment for military services continually shifts, the Marine Corps will be required to scope and implement software-based solutions at the edges of the battlefield. These solutions will have to function without connectivity or assistance from centralized or contracted support.

MCSWF's initial subjects will undergo a three-year program consisting of three phases: a technical accelerator, one-to-one pairing enablement, and employment utilization. Matthew Glavy, Marine Corps' Chief Information Officer Lt. Gen., will serve as the MCSWF's executive sponsor. "The Marine Corps Software Factory is about outcomes, creating an advantage for Marines at the tactical edge, today," said Glavy. "The MCSWF will provide viable capabilities to enhance mission readiness through the power of information."

Belkin International, Inc.
555 S. Aviation Blvd, Suite 180
El Segundo, CA 90245 USA

belkin.com/cybersecurity

Support
Secure SKVM/SKM Support 800-282-2355

Sales
FederalBusinessDivision@belkin.com

Learn more about
Belkin's cybersecurity solutions.