Viasat

Transitioning to Next-Generation Hardware

BEYOND Encryption

THE NEXT CHAPTER OF HIGH ASSURANCE

Why Transition Now?

- Rapid advances in computing and cryptanalysis are reshaping the threat landscape.
- Long-deployed high-assurance hardware faces growing risk as adversary capabilities evolve.
- Proactive modernization is essential to protect U.S. and allied classified communications.

The Shift Ahead

Establishing a Foundation for Continuous Threat Resistance

- Transition legacy high-assurance encryption devices to next-generation hardware platforms.
- Enable incremental NSA-driven upgrades on a path toward future-ready cryptography.
- Extended operational lifespan while maintaining mission assurance.

What Customers Need to Consider

Key Considerations for a Successful Transition

- Infrastructure realities matter - bandwidth, connection types, and deployed environments vary.
- Physical constraints such as size, power, mounting, and connectors must be planned early.
- Scalability, sustainment, and long-term vendor support are critical to mission success.

Transition Models

Managed vs. Discretionary Transitions

- Device modernization is not a one-size-fits-all effort.
- Program-level operational needs and approval pathways differ across missions.
- Successful transitions account for unique operational, management, and Approval to Operate requirements.

Overcoming Structural Challenges

Navigating Centralized Procurement Limitations

- Improve early alignment between program requirements and encryption vendor capabilities.
- Evaluate ordering, delivery, sustainment, and factory return processes holistically.
- Consider vendors that enable greater depot-level self-sufficiency and long-term resilience.

We're here to help you prepare

Learn more at **viasat.com/beyondencryption**, contact **insidesales@viasat.com**, or call **888.842.7281**