TACLANE®-MultiBook Secure Laptop

Incredibly Secure — Decidedly Mobile

Overview

The TACLANE-MultiBook secure laptop is the only “all in one” solution for mobile classified computing. Mobile users can now use this commercial laptop to remotely and simultaneously access unclassified and classified information. The MultiBook’s integrated security protects data stored on the computer, as well as data being sent to and from networks classified Secret and below.

Availability

NSA certified and available.

Applications

The TACLANE-MultiBook is ideal for:

- Telecommuters and road warriors
- First responders
- High-risk environments
- Fixed and mobile secure facilities
- Covert mobile users
- International travelers
- Multilevel computing users

Complete Mobile Classified Computing Solution

NSA certified Suite B Security

Integrated TACLANE® HAIPE® data-in-transit and ProtecD@R® data-at-rest encryption

Simultaneous access to unclassified, NIPRNET and SIPRNET networks

All the features of a commercial laptop

No COMSEC handling and transportation requirements
**Multiple Features in a Single Solution**

**Latest Computing Features**
- Dell Latitude E6430
- Wide range of available computing options and accessories including: docks, monitors, keyboards and mouse, wireless adapters, input devices and CAC/PIV readers
- Accommodates standard COTS USB devices (may be mapped to specific domains) for flexibility and future expansion
  - USB network adapters
  - USB removable media (e.g., USB CD/DVD drives and USB thumb drives)
  - ExpressCard devices are supported provided they only use the USB portion of the ExpressCard interface
- Operating Systems Supported
  - Microsoft® XP, Vista®
  - Microsoft Windows 7

**Security**
- Designed for Secret and below with non-CCI CHVP handling
- Proven TACLANE HAIPE® v3.0.2 encryption for Data-in-Transit protection

**ProtecD@R®** Data-at-Rest encryption for Secret and below
- Field zeroize
- Data recovery
- Tamper evident solution
- Field software/firmware upgradeable
- Cryptographic token for access control of all cryptographic functions
- Permits simultaneous communication with Secret and unclassified networks
- Key management:
  - Authenticated PPK for HAIPE Data in Transit (DIT)
  - No key management necessary for Data at Rest (DAR)

**Secure Virtualization**
- Simultaneous view of multiple security levels, domains and operating systems with TVE trusted data separation

**Operational Environment**
- Operates in non-secure environments over public networks
- Connects directly to Secret and unclassified networks in secure environments (office or garrison)

**Network Connectivity**
- High over Low Tunneling
  - Secure access to Secret and below networks via HAIPE® tunnel across non-secure public networks
- TVE/High Assurance Platform® (HAP) architecture allows initial access to public networks before going secure, without the need to reboot
- Connectivity in office or garrison is provided through independent red and black network interfaces
- Wireless connectivity to unclassified networks via COTS networking capabilities like cellular and WiFi
- MCEP and VPN Connectivity
- Network interfaces for encrypted classified and unclassified use
  - Integrated Fast Ethernet LAN (copper)
  - 802.11 b, g and n via external USB WLAN adapters
  - Cellular via external USB WWAN adapters
- Plaintext data network interface for direct connection to classified networks

**Handling**
- Transported as a Cryptographic High Value Product (CHVP)
- Simplified Transportation and Accounting per CHVP Policy CNSSI No.4031
- Tamper Case enhances security and eases handling
  - TSA friendly
  - Safe for shipping and storage
  - Enables Non-CCI handling

---

**Security module**

**Tamper case**