CSfC for Data at Rest Data Sheet

As data at the edge faces high vulnerability, the NSA's Commercial Solutions for Classified (CSfC) program sets stringent requirements to protect classified information. To ensure sensitive data is secured from malicious actors, NSA requires layered protections. Cigent, with its drive partners, is a leading provider of CSfC-compliant Data at Rest (DAR) solutions.

CSFC FOR DAR

- **Single Solution:** Cigent firmware and PBA is integrated seamlessly with DIGISTOR Citadel C Series Advanced or Seagate Barracuda 515 drives.
- **AES-256-bit Full Drive Encryption:** proven AES 256-bit encryption methodology using maximum characters that has been validated by NSA, CISA, and other experts
- **Pre-Boot Authentication (PBA):** encryption is supplemented by pre-boot authentication (PBA) providing an additional outside layer of protection that certifies credentials before the system can boot the drive. This eliminates the risk of the hard drive from being read before credentials are entered.
- **Multifactor Authentication (MFA):** Optional configuration with PBA provides MFA capability requiring use of both U/N Password and smart card (CAC).

Cigent Difference

- **Validation by Experts:** Cigent was developed for and with leading US Federal agencies leading Federal agencies including MITRE, NIST, NSA, NIAP, the Air Force, Cyber Resilience of Weapon Systems (CROWS).
- **Robust Ecosystem:** Cigent has active relationships with all major CSfC integrators including AFRL, Booz Allen, CACI, and Exerfox to enable your mission requirements.
- **Device Partnerships:** Cigent Secured Storage solutions are available from device and computing manufactures including Dell, HP, and GETAC.

ADMINISTRATION

- **Enterprise Management Console:** Deployable in the cloud or on-premises for comprehensive key management, compliance reporting, and policy setting.
- **Command Line Interface (CLI):** Available for both Linux and Windows, streamlining deployment automation.

ENHANCED SECURITY CAPABILITIES

Cigent Secure Drives address additional data protection requirements with unique features.

- **Prevent Cloning and Wiping:** Full drive encryption and hidden partitions lock all ranges preventing malicious compromise. Data secured within hidden partitions remain unreadable even if the device is in use.
- **Data Erasure:** nitiate data erasure command locally or remote with crypto and full block wipe. Can be used for emergency situations or to repurpose drives.
- **Secure Data Logs:** Cigent captures every data transaction in secured, tamper-proof logs. Can be used to detect malicious insider activity and provide valuable forensics.

Secure Your Data

- Cigent's CSfC DAR solutions deliver exceptional data security at the edge, backed by a dedicated team ensuring mission success with minimal disruption. Our combination of validated drives, extensive partner ecosystem, and additional protection capabilities sets us apart.

Schedule a Demo with Us to Learn More!