CIGENT
AlwaysPROTECTED™

PROTECTED DATA AT THE EDGE
Protecting your data, enabling your mission

CSfC for Data at Rest Data Sheet

The NSA Commercial Solutions for Classified (CSfC) program defines requirements for protecting classified information on devices operating at the edge. Meeting CSfC for DAR compliance requires hardware encryption, software encryption, and software authentication and management.

Cigent provides a single integrated solution to meet CSfC for DAR requirements. The proven solution includes both inner and outer-layer protection, enabling compliance and ensuring sensitive data is protected from unauthorized access.

Layered Protection

Outer-Layer Protection

- **Hardware AES-256-bit Full Drive Encryption**: proven AES 256-bit encryption methodology validated by NSA, CISA, and other experts.
- **Pre-Boot Authentication (PBA)**: encryption is supplemented by NSA-validated PBA. PBA provides a separate, secure environment that certifies credentials before the system can boot the drive.

Inner-Layer Protection

- **Software Full Drive Encryption (FDE):** an additional inner layer of encryption utilizing separate cryptography maintains protection following hardware boot.
- **Multifactor Authentication (MFA):** users authenticate unlocking FDE with MFA capability requiring the use of both U/N Password and smart card (CAC) or security key.

Efficient 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.

Proven Solution

- **Validation by Experts:** The solution has been extensively tested and is validated by Federal agencies including MITRE, NIST, NSA, NIAP, USAF, and Cyber Resilience of Weapon Systems (CROWS).
- **Robust Ecosystem:**
  - Extensive relationships with all major CSfC integrators including AFRL, Booz Allen, and CACI to enable your mission requirements.
  - The solution is available directly from device and computing manufactures including Dell, HP, and GETAC.

CIGENT
AlwaysPROTECTED™

PROTECTED DATA AT THE EDGE
Protecting your data, enabling your mission

Enhanced Security Capabilities

Cigent Secure Solutions provides advanced data protection features to address critical data security use cases.

- **Hidden Partitions:** Option to create undetectable partitions that are unreadable at the sector level. Adversaries cannot detect drive or data, preventing data attacks, including cloning and wiping.
- **Data Sanitization**: Local or remote activation of crypto and block erasure coupled with patented block-by-block erasure verification. Provides emergency data sanitization or allows drives to be repurposed or reused.
- **Insider Threat Protection**: Secure Logs capture every data transaction in secure, tamper-proof logs. These logs can be used to detect malicious insider activity and provide valuable forensics.

Secure Your Data

A single solution enables organizations to meet compliance standards with layers of protection to prevent unauthorized data access. With cleared personnel (TS/SCI) and decades of DoD and IC mission experience, the team stands ready to support your mission requirements.

Learn more at Cigent.com or request a demo of our CSfC for DAR solution.

CIGENT
AlwaysPROTECTED™

Cigent provides unparalleled technology, ecosystem, and expertise to ensure your sensitive data is protected no matter what your mission. The Cigent solution was developed for and with US Federal agencies by leading experts in data recovery and sanitization. Cigent is a trusted partner in addressing your data protection at the edge requirements. We will work with you to understand your mission requirements and ensure you have data protection that will enable your success.

Book a Demo