Understanding CSfC for Data at Rest

The NSA Commercial Solutions for Classified (CSfC) program defines requirements for protecting classified information on devices operating at the edge. A "certified" SSD self-encrypting drive (SED) is a necessary element, but alone, it is insufficient to meet compliance. Meeting CSfC for DAR compliance requires hardware encryption, software encryption, and software authentication and management.

CSfC for DAR is required for desktops, laptops, and servers with classified data.

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.

Administration

An additional consideration is the administration of the protection. Management includes deployment, key management, policy setting and compliance reporting and audit capabilities.

The solution will be ineffective and will not meet compliance without proper configuration and reporting. In selecting a CSfC DAR solution, it is ideal if it offers enterprise management and a command line interface to streamline administration.

Considerations

The selection of a technology partner should take into consideration several elements:

- Select a single integrated solution that includes both the inner and outer layers of protection. Ensure that independent crypto libraries are used for hardware and software encryption layers.
- RAID server deployments provide valuable performance and resiliency benefits. Select a technology provider whose solution can protect data on RAID without impacting performance.
- Enterprise administration will expedite deployment and streamline policy requirements.
- Ensure the solution is validated by and supported by major CSfC integrators including AFRL, Booz Allen, and CACI.
- Simplify procurement by selecting a vendor whose solution can be

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