Why TAA, FIPS, and Common Criteria should Matter in Federal System's Security Architecture

By Mike Moritzkat, CEO and Managing Director, Seagate Government Solutions

Now, more than ever, enhanced data security is a necessity for government agencies and contractors. They must go beyond safeguarding systems—security must start at the data storage device (HDD/SSD) level.

If one considers the drive an element of the overall security architecture by leveraging the security functionality and features of the drives, they can be so much more. A technical director in one of our intelligence agencies was the first to fully recognize the benefits, fueling the agency's interest in working more closely with Seagate Government Solutions.

Trade Agreements Act (TAA), Federal Information Processing Standards (FIPS) and Common Criteria (CC) compliant drives provide a validated encrypted data-at-rest storage capability that provides enterprise owners a high-assurance means to protect their data. These security features that are built into the drives can be highly leveraged by security architects, if they truly know and understand these unique capabilities.

For example, Hardware Root of Trust is a "random" key generated and inserted during wafer fabrication and is unique to every device. The random number generator is NIST 800-90A compliant and the hardware root key cannot be changed without destroying the drive—a powerful security feature. Secure Crypto-Erase provides a mechanism to eliminate, in an absolute manner, access to any data resident on the drive in emergency instances making the data non-recoverable. Combining the ability to individually encrypt drive segments enables versatility in multi-use environments.

Seagate is continuing its engagement with Federal Agencies on what security features exist and how they can be used in order to help facilitate an understanding on the value of using TAA FIPS CC drives. Once the security properties are understood, these advanced security features will provide the security architect the highest possible assurance for the overall system.

Seagate is a pioneer and leader in the TAA and Common Criteria storage device market thereby enabling compliance with Government Contract requirements. Seagate's encrypted HDDs and SSDs are also validated to comply with FIPS 140-2 Level 2 standard. The Federal Information Processing Standard 140-2 coupled with Common Criteria combine in the validation of the Crypto-erase feature. Seagate's hardware root of trust and many other firmware protection characteristics ensure that only authorized and authentic firmware is loaded on the drives during manufacturing and upon boot-up in the End User's system.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide certification program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based products and services for Federal Agencies or CSP's that want to host a Federal Agency's data. Seagate has created the industry's first storage-related FedRAMP Security Control documentation in official FedRAMP templates for its HDD's, SSD's and Enclosures, which can be used by any Federal Agency and/or CSP as part of their own overall FedRAMP System Security Plan (SSP).

Federal Agencies now have options in adopting the use of TAA, FIPS 140-2 devices, and Common Criteria drives in their IT, Cloud and other systems, IT systems and cloud architectures. This ensures a solid security posture, adherence to all Federal security mandates and standards, and saving capital—both human and monetary. For more information contact us at inquiries@seagategov.com.

About Seagate Government Solutions

Seagate Federal Inc., doing business as Seagate Government Solutions, is a wholly owned FOCI mitigated subsidiary of Seagate US Holding Inc. and sister company of Seagate Technology LLC. Located in the Washington DC metropolitan area, SGS is dedicated to forwarding the technology of Seagate while solving the security and storage needs of the US Federal Government and it partners.