FOR IMMEDIATE RELEASE

Cigent Patents Technology that Ensures Complete Erasure of Storage Drives and Endpoint Devices

80% of wiped device still retain potentially sensitive data

March 21, 2023, Ft. Myers, FL – Cigent® Technology, Inc., the leader in embedded cybersecurity in storage devices, today announced that they have been assigned a patent (11581048) developed by Tony Fessel, VP of Engineering, Fort Myers, FL, for "method and system for validating erasure status of data blocks."

Organizations have a responsibility to always protect data on endpoints, including when they are transitioned from one employee to another, are retired, or donated to charities. Failure to protect sensitive and critical data including PII, intellectual property, trade secrets, and classified information is a violation of laws including HIPAA, GDPR, and CCPA, and is a risk to national security.

IT leaders know this and take data removal seriously when a device is being repurposed or EOLed. Before endpoints and drives are transitioned, IT leaders follow industry best practices to wipe drives using technologies such as ATA Security Erase or paying for managed services to perform certified drive wipes. Storage devices provide a response indicating the erase command was completed successfully, in theory, wiping all data.

Research by CPR Tools determined that 42% of Solid-State Drives had recoverable sensitive (not just PII) data on them. As a result of this type of research, the NSA issued guidance requiring SSDs to be destroyed.

Drives can falsely report that the data was wiped due to incorrectly implemented commands, bad sectors, hardware failures, erasure program failures, human error and more. An additional challenge, specifically with SSDs, is wear leveling and the need to have additional blocks to move data around that are often not scanned when an erasure verification command is issued.

To address these gaps, Cigent's patented technology is now included in its Verified Device Erasure, firmware-based verification capability. Verified Device Erasure scans the complete Storage SSD to verify the type of data and whether it has been erased. It then displays a report for the user showcasing results.

"Cigent Verified Device Erasure is the only reliable method to verify that an SSD has truly been erased and can be safely repurposed," said Tom Ricoy, CRO at Cigent.

Cigent Secure SSD™ drives, originally developed for U.S. government and military use, are the world's first commercially available cyber-secure SSDs and are being implemented by key hardware partners. Drives that feature Cigent Verified Device Erasure, are the only drives listed on the NIAP common criteria certified product list.

Cigent Secure SSDs with Verified Device Erasure are sold by Cigent and multiple storage manufacturers including Seagate Government Solutions (Barracuda 515), DIGISTOR (Citadel C Series Advanced), Kanguru, and Envoy Data. They are available in both FIPS validated and NIAP Common Criteria certified storage devices. Secure SSDs are available from leading distributors TD Synnex, Carahsoft, and ImmixGroup and on multiple federal and SLED contract vehicles including GSA, NSA SEWP, NCPA, Texas DIR, Maryland COTS, and Pennsylvania COSTS.

About Cigent
Cigent offers a new approach to data security for organizations of all sizes to stop ransomware and data theft, as well as achieve compliance. Cigent protects your most valuable asset - your data - against the most sophisticated adversaries. We protect data throughout its lifecycle via prevention-based defenses embedded into storage and individual files. From decades of data recovery, cybersecurity, and device sanitization experience, the experts at Cigent have developed prevention methods beyond anything that exists today. Cigent.com.

Contact:
Ashley Justiniano
914 391 3516
ajustiniano@mww.com