blancco

Data Erasure at Every CMMC Level

How Blancco Helps U.S. Defense Contractors Fulfill Media Sanitization Requirements

U.S. defense contractors handle a lot of government data, and a new certification framework is being rolled out to make sure that data is protected.

The Cybersecurity Maturity Model Certification (CMMC) framework confirms an organization's ability to protect FCI (federal contract information) and CUI (classified uncontrolled information). Instead of the previous method of relying on organizations' self-assessments, third-party assessors evaluate contractor competencies across five levels of cybersecurity maturity.

The good news is that Blancco's globally certified data erasure solutions and audit-ready reports equip you to follow all of the CMMC's media sanitization requirements across an incredibly wide set of data storage devices. This comprehensive approach provides operational efficiency, consolidated support and training, and centralized reporting to verify compliance.

CMMC Media Sanitization Requirements by Domain

Each of the five CMMC levels incorporates sets of processes and practices distributed over various domains. The Media Protection domain requires FCI sanitization and applies to all five levels. The Asset Management and Maintenance domains require CUI data sanitization at the three most advanced levels. Requirements as listed in the CMMC Appendices are outlined on the following pages.

blancco

CMMC REQUIREMENT	HOW BLANCCO HELPS
Level 1. Basic Cyber Hygiene **Domain:** Media Protection (MP) **Practice:** MP.1.118: Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. **Discussion Points** "This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. [Digital] examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices..." "NIST SP 800-88 provides guidance on media sanitization."	With Blancco's software-based data erasure, you can safely and confidently dispose of, reuse, or resell virtually any digital media storage device. Not only does this reduce the amount of e-waste sent to the landfill, it also provides an opportunity to increase returns on your technology investment. Fully compliant with NIST SP 800-88 media sanitization guidelines, Blancco can immediately erase active or inactive data across a comprehensive variety of IT assets, including: • PCs and laptops (including Apple devices) and other hard drive-containing assets such as enterprise-grade scanners, copiers, and printers • Loose drives (HDDs and SSDs, including NVMes) • Servers, LUNs and VMs • Network devices (routers, switches, access points) • Mobile devices, including smartphones and tablets (iOS, Android) • Removable media Blancco software can also target no-longer-needed files and folders for removal through automated, policy-based processes. All erasures are verified and result in a tamper-proof, digitally signed, and audit-ready report to prove compliance with CMMC sanitization requirements. These reports, or "Certificates of Erasure," provide clear documentation of which devices were erased, when, by whom, according to what standard, and more.
Level 3. Good Cyber Hygiene **Domain:** Asset Management (AM) **Practice:** AM.3.036: Define procedures for the handling of CUI data. **Discussion Points** "The organization should define procedures for the proper handling of CUI. These procedures typically involve establishing controls to protect and sustain sensitive information. Examples of controls an organization may implement through data handling procedures include policies (data categorization, protection, disposal, backup), access controls for data, regular backups and physical security protections.	Whether you're erasing devices that have been used to store CUI or erasing specific files, Blancco helps you proactively and consistently carry out CUI data disposal policies throughout your IT infrastructure. **Automated Workflows & ERP/AMS Integrations.** The Blancco Secure Data Erasure app provides full control of asset erasure within the ServiceNow environment. Outside of ServiceNow, our two-way communication integrates Blancco solutions with your existing asset management system (AMS) and enterprise resource planning (ERP) software. Both allow you to execute computer and data center erasures remotely, verify erasures, and ensure repeatable procedures that comply with your CUI device disposal policies. **Policy-Based Automations.** Blancco File Eraser's policy-based automations facilitate end-of-life CUI data erasure on servers and devices across your network. Command line options automate secure file erasure through scripting, ensuring that security and data management policies, including NIST Clear or Purge sanitization, are correctly followed. Blancco File Eraser also combines with Microsoft File Classification Infrastructure for erasure based on classification rules and properties you set up. **Audit-Ready Documentation & Reporting.** Centrally stored, customizable, and audit-ready reports document the processes followed for each erasure and verify that data sanitization has indeed occurred.

blancco

CMMC REQUIREMENT	HOW BLANCCO HELPS
Level 3. Good Cyber Hygiene **Domain:** Maintenance (MA) **Practice:** MA.3.115: Ensure equipment removed for off-site maintenance is sanitized of any CUI. **Discussion Points** "This requirement addresses the information security aspects of system maintenance that are performed off-site and applies to all types of maintenance to any system component…" **CMMC Clarification** "Sanitization is a process that makes access to data infeasible on media such as a hard drive. The process may overwrite the entire media with a fixed pattern such as binary zeros. In addition to clearing the data an organization could purge the data, or even destroy the media. By performing one of these activities, the data is extremely hard to recover, thus ensuring its confidentiality." Refers to NIST SP 800-88R 1 for guidance.	Easily deployed on premises, Blancco data erasure securely overwrites digitally stored information with random binary data according to a specified standard (e.g., NIST Clear or Purge), then verifies and certifies that the erasure has been successful. For Purge-level sanitization on HDDs and SSDs, Blancco Drive Eraser reaches all sectors of the device, even removing hidden areas such as host protected areas and device configuration overlays, then executing firmware-based commands specific to the type of drive. Clear and Purge sanitization can also be applied to a range of data storage devices, including network devices such as routers and switches and mobile devices such as smartphones and tablets. These procedures render all data permanently unrecoverable while preserving the functionality of the device being sent out for repair.

Discover how the world's leading data erasure software ensures compliance with CMMC data sanitization requirements. Sign up today for your **free enterprise data erasure trial**.