



CMMC

MEDIA PROTECTION

Always Encrypted. Always Accounted For.

Media Protection makes sure anything that can carry data (e.g., USBs, external drives, DVDs, portable laptops, even printed pages) is controlled, encrypted, tracked, and sanitized. So when data moves, it doesn't escape.

Proof of Practice

Examples

- ✓ **Encryption Evidence**
Device list showing encryption status for laptops and approved USBs, plus screenshots of BitLocker/FileVault settings.
- ✓ **Media Log & Labels**
Checked-in/checked-out registry for company media with asset tags and "CUI - Encrypted" labels photographed.
- ✓ **Sanitization Records**
Short forms documenting method (clear/purge/destroy), tool/version, serial numbers, date, and sign-off.

The Business Impact

One misplaced, unencrypted thumb drive can expose CUI, trigger reporting, and jeopardize contracts. Strong media protection builds customer trust, protects your reputation, and proves you're a reliable link in the DoD supply chain.

Available Resources

-  **NIST SP 800-88: Guidelines for Media Sanitization**
<https://csrc.nist.gov/pubs/sp/800/88/r2/final>
-  **CISA Tip Sheet: Removable Media Best Practices**
<https://www.cisa.gov/resources-tools/training/how-protect-data-stored-your-devices>
-  **DCSA CUI Marking Job Aid**
<https://www.dcsa.mil/Portals/91/Documents/CTP/CUI/21-10-18%20CUI%20MARKING%20JOB%20AID%20FINAL.pdf>
-  **Microsoft Intune: Device Management**
<https://www.microsoft.com/en-us/security/business/microsoft-intune>
-  **Jamf: Apple Device Management**
<https://www.jamf.com/>

Quick Wins

-  1. Turn off unapproved USB storage (via GPO/MDM)
-  2. Encrypt every portable drive & laptop
-  3. Issue approved, labeled media only
-  4. Create a simple sign-out log for media
-  5. Sanitize media before reuse/disposal