Handling, Transporting and Destroying Digital & Physical Media Policy

811.1 PRINTED MATERIAL

Printed material may be placed in Confidential Destroy bins and subsequently destroyed by an approved contracted vendor. Some units have their own confetti shredders that they may use. "Strip cut" shredders are not to be used for CJI or other confidential data.

811.2 ELECTRONIC MEDIA

Electronic records on decommissioned servers or other storage devices are to be securely erased using DOD approved methods or the physical media destroyed. Electronic media may be reused; however, the media should be securely erased first where practical.

- CD/DVD Media
  - Break/destroy media prior to disposal
- Hard Drives
  - Erase the drive using DOD approved methods
  - Use approved vendor provided utility for built-in "secure erase" function
  - Break/destroy the hard drive (drill several holes through platters, shred, smash to point where platters and PCBs are broken)
- Tapes
  - Erase using DOD approved methods (degauss)
  - Destroy (shred)
- Flash Drives
  - Break/destroy the device

Electronic media may be placed in Confidential Destroy bins where an approved vendor destroys them for us.

811.3 TRANSPORTATION

Printed material, electronic media, or containers with CJI may only be handled or transported by approved persons who have been finger print background checked.

- Digital Media Transport
  - Only authorized employees shall transport media and shall protect and control said media when moving it from a controlled area to prevent any compromise of the data.
- Physical Media Transport

- Only authorized employees shall transport media (printed documents, photos, etc.) and shall protect and control said media at the same level as electronic form when moving it from a controlled area o prevent any compromise of the data.

811.4 STORAGE AND ACCESS

Printed material, electronic media, or containers with CJI may only be stored at approved locations staffed by persons who have been finger print background checked. Department personnel shall store digital and physical media within physically secure and controlled areas. Access to digital and physical media is to be limited to authorized individuals. If physical and personnel restrictions are not feasible then the data should be encrypted.