

Removable Media Destruction

May 2012



ON CYBER PATROL



With the ease of use and technological advances, the quantity of removable media in the government and military is increasing. Removable media refers to storage media that is designed to be removed from the computer without powering the computer off. Removable media comes in many forms, but typically includes CD/DVD, secure digital (SD) cards, tape, flash drives and multimedia cards. Removable media often contains sensitive bits of information, which should not be just thrown away. Regulations regarding paper documents also include the different types of removable media, and your organization should incorporate removable media into its records management program and retention schedule.

We have all heard the saying "One man's trash is another man's treasure". However, this has never been a more true statement than it is right now. Removable media has made our lives much easier due to the technological advances that have taken place. We no longer carry around large, bulky external storage media devices or numerous CDs in order to transport data. With the sizes being reduced to that of a key chain or smaller, we must ensure we don't throw flash drives away with regular office trash. Long gone are the days of seeing large piles of ADP equipment waiting to be hauled to the dump. This technological advance requires proper tracking and disposal of media that may otherwise be overlooked.

Now that the weather has changed and spring has finally arrived we find ourselves conducting spring cleaning both around the house and in the office. In our desire to reduce clutter we must remain cognizant about the requirement to properly dispose of our removable media. Properly disposing of removable media is one of the key ways we can keep our enemies from gaining the advantage. Most removable media allowed to be used on Information Systems (IS) by the Department of Defense (DoD) is required to be encrypted to avoid the risk to sensitive data in the event of loss or theft. Encryption is a procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process. Many users believe that once information is encrypted on a piece of media it can no longer be accessed.

While encryption does add an extra layer of protection, it does not take the place of proper disposal/destruction procedures. Users should be trained to understand that even when data is encrypted it still poses a risk. There are un-encryption tools readily available to our adversaries, which allow them to access encrypted data.

There are a number of approved methods to destroy removable media that can be found in AR 25-2 and AR 380-5. Some of the approved methods include burning, shredding, pulping and pulverizing. Users should turn over all removable media for destruction to their security POC. Following proper disposal/destruction procedures not only safeguards personal identifiable information from falling in the hands of hackers and identity thieves, but it also keeps our country safe from those with more sinister plans.