Ghosting or Cloning Accredited Information System

Cloning, also known as disk imaging or ghosting, computer hard drives has been used by Information Technology (IT) professionals for years as an invaluable tool in the corporate unclassified environment. Creating a clone of the corporation's "standard configuration" makes replacing damaged hard drives or recovering from a user accidentally deleting valuable applications, an almost effortless task. It also provides consistency in configuration management to prevent addition of non-approved applications. This technology can also be used to provide efficiencies within the classified processing environment.

NISPOM Chapter 8 requires the Information System Security Manager (ISSM) to review and certify to the accrediting Cognizant Security Agency (CSA) that all systems have the appropriate protection measures in place and validate that they provide the protection intended (NISPOM 8-201). Traditionally, the ISSM provides their certification for every Information System (IS) to the CSA in a cover letter with the accompanying System Security Plan (SSP), or by signing each individual revision log or certification test guide. The ISSM is certifying that they, or the ISSO (Information System Security Officer), has tested (NISPOM 8-614) all security features, including access controls and configuration management, for every IS they are submitting to the CSA for accreditation. Disk cloning is an alternative process to accomplish the same goal while decreasing the time required by the ISSM/ISSO to build multiple classified processing systems, minimizing the potential for misconfiguration through human error and reducing testing/certification time of security features on each individual cloned system.

Almost every major computer vendor, to include dozens of companies that specialize in providing resource or security related utilities, has a process or utility for cloning hard drives. Though not without some potential problems, this technology has matured to where replicating exact system configuration settings on hard drives to be used in a classified environment is permissible and recommended. Countless hours of IT resources can be saved and security can be enhanced by using a reliable cloning utility and by following a documented process.

Procedures for Creating and Verifying a Cloned Image

1. The ISSM will develop written procedures for cloning, installing and testing images that are 100% NISPOM Chapter 8 compliant. These procedures will be maintained as part of the configuration management process and must address revision control.

2. The ISSM or ISSO will build and certify a system that is 100% NISPOM Chapter 8 compliant based on the applicable protection level and approved security plan. This system will serve as the approved system image for cloning.

3. The cloned image is created on recordable media using a non-rewritable format.

4. The first cloned system is built and all security features and system settings are verified to be functioning.

5. A SHA-1or equivalent, checksum of the cloned image is created.

6. Provided the cloned image does not contain any classified data, the media shall be labeled "UNCLASSIFIED—FOR MAINTENANCE ONLY"" and protected in accordance with procedures identified in the SSP (NISPOM 8-304b(4).

The cloned image can now be reproduced for distribution or sent via normal unclassified emailed. If reproduced, the SHA-1or equivalent checksum shall be written to the media label. If sent via normal unclassified email, the checksum must be sent in a separate email. The receiving ISSM or ISSO will build a new system from the cloned image and run another secure hash checksum. The checksum from the new system will be compared to the checksum from the original cloned image. If the checksums compare, an entry in the maintenance log is recorded and the certification requirement is met. If the checksums do not compare, the ISSM or ISSO that sent the cloned image will be notified.

Cloned images do not:

- Replace the need for approved system security plans,
- Negate the need to configure IS security settings not automatically configured in the cloned image to meet NISPOM requirements i.e. Bios settings.
- Negate the NISPOM requirement that the local ISSM be competent to the level of complexity of the systems they manage,
- Infer any approval for accreditation or self certification outside of an approved Master System Security Plan,
- Negate the requirement for annual self inspections,
- Negate the requirement for a signed statement by the ISSM that the system complies with the requirements of the protection level and levels of concern for the system, or
- Negate the requirement for Certification Test Plans.

NOTE: Sales of off-the-shelf software products are normally supported by shrink-wrap and "click-to-accept" licensing agreements. Many come with restrictions such as hardware, office location and purpose of use. Product acceptance terms are often a very important issue. Warranty provisions are critical as well as implementation schedules, payment terms and confidentiality provisions. Please read all software licensing agreements and ensure that you are in compliance with the terms of the agreement before you begin cloning.