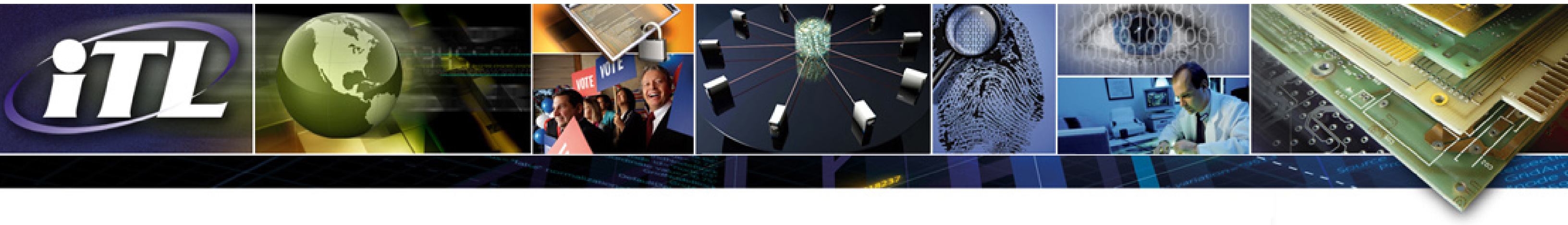


ITL BULLETIN FOR FEBRUARY 2015

NIST SPECIAL PUBLICATION 800-88 REVISION 1, *GUIDELINES FOR MEDIA SANITIZATION*

Andrew Regenscheid, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

NIST has published an updated version of Special Publication (SP) 800-88, *Guidelines for Media Sanitization*. SP 800-88 Revision 1 provides guidance to assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information. Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. Information disposition and sanitization decisions occur throughout the information system life cycle.

The publication states that the types of media used to create, capture, or transfer information used by the system should be determined during the requirements phase of the system. This analysis, balancing business needs and risk to confidentiality, will formalize the media that will be considered for the system to conform to Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*.

Media sanitization is one of the key elements in assuring confidentiality. In order for organizations to have appropriate controls of the information they are responsible for safeguarding, they must properly secure used media.

SP 800-88 Revision 1 recommends processes to guide media sanitization decision making regardless of the type of media in use. To effectively use this guide, organizations and individuals should focus on the information that may have been stored on the media, rather than focusing on the media itself. The document also includes guidelines and recommendations on methods for sanitizing different types of media, as described below.

Types of Sanitization

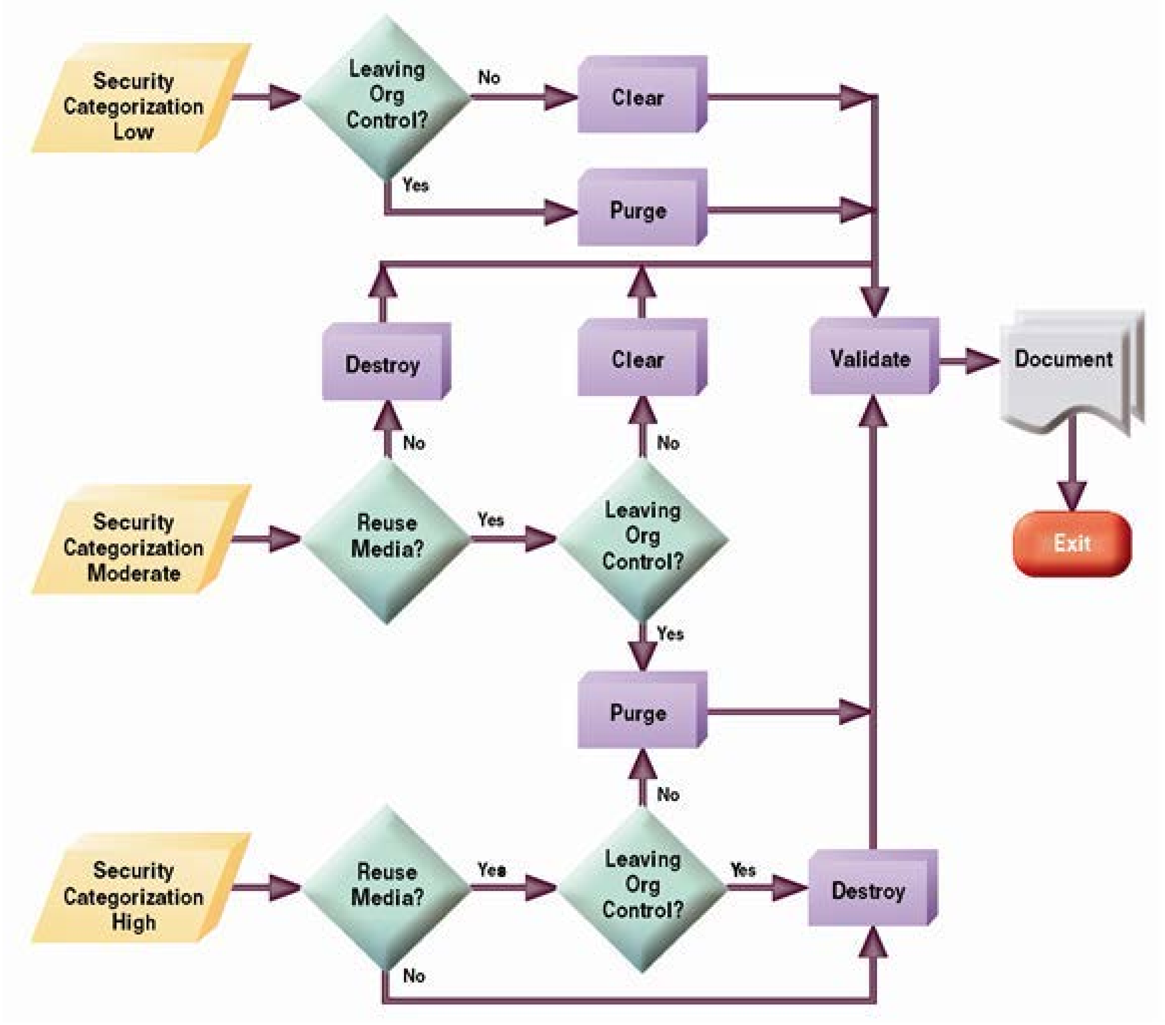
The publication describes three types of media sanitization – Clear, Purge, and Destroy - that can help ensure that data is not unintentionally released. These types are defined as follows:

- **Clear** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple noninvasive data recovery techniques; it is typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).

- **Purge** applies physical or logical techniques that render target data recovery infeasible using state-of-the-art laboratory techniques.
- **Destroy** renders target data recovery (using state-of-the-art laboratory techniques) infeasible and results in the subsequent inability to use the media for storage of data.

Sanitization methods for specific media/device types are provided in Appendix A of the document.

Organizations using this guide should categorize the information to be protected, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. Then, the organization can choose the appropriate type(s) of sanitization. The **chart below** provides a decision process flow to assist organizations in making sanitization decisions that are commensurate with the security categorization of the confidentiality of information contained on their media. This decision process is based on the confidentiality of the information, not the type of media. Once organizations decide what type of sanitization is best for their individual case, then the media type will influence the technique used to achieve this sanitization goal.



Verification Methods

The publication recommends two types of sanitization verification. The first is to perform verification every time sanitization is applied. The second is a representative sampling verification, applied to a selected subset of the media. If possible, the sampling should be executed by personnel who were not part of the original sanitization action. The goal of sanitization verification is to ensure that the target data was effectively sanitized. SP 800-88 Revision 1 provides different methods of verification based on destructive techniques that have been used.

Trends in Data Storage Media

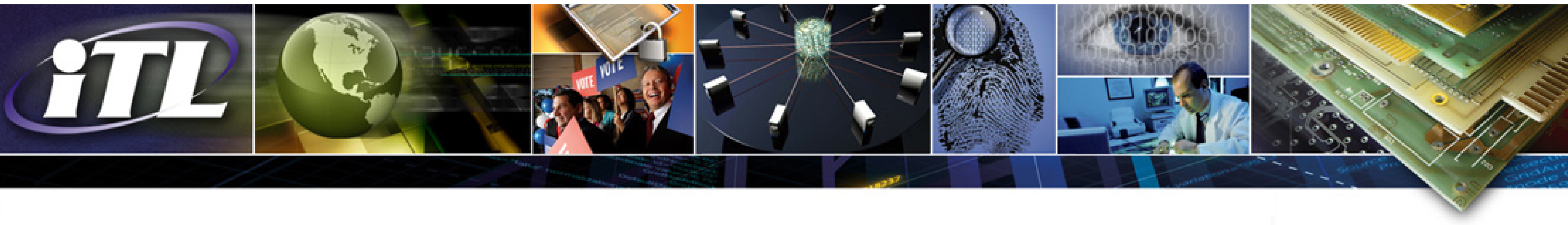
SP 800-88 Revision 1 provides analysis of trends in growing storage capacity and describes revolutionary and evolutionary changes in sanitization. The publication mentions that media technologies, such as flash memory-based storage devices including Solid State Drives (SSDs) and self-encrypting drives, have become prevalent. Degaussing and overwriting techniques - common methods for sanitizing magnetic media - are not applicable for flash memory devices. Evolutionary changes in magnetic media also have impacts on sanitization. New storage technologies, and even variations of magnetic storage, are dramatically different from legacy magnetic media. These clearly require sanitization research and a reinvestigation of sanitization procedures to ensure efficacy.

Trends in Sanitization

The publication summarizes some trends in sanitization. For storage devices containing *magnetic* media, a single overwrite pass with a fixed pattern, such as binary zeros, typically hinders recovery of data even if state-of-the-art laboratory techniques are applied to attempt to retrieve the data. One major drawback of relying solely upon the native Read and Write interface for performing the overwrite procedure is that areas that are not currently mapped to active areas (e.g., defect areas, over provisioned, unallocated space) may not be securely sanitized. These native methods also may not reliably overwrite all areas when wear-leveling techniques (commonly used with flash memory) are employed. Dedicated sanitization commands may support addressing these areas more effectively, but also require a level of assurance from the vendor.

Destructive techniques for some media types may become more difficult or impossible to apply in the future. Traditional techniques such as degaussing (for magnetic media) become more complicated as magnetic media evolves, because some emerging variations of magnetic recording technologies incorporate media with higher coercivity (magnetic force). As a result, existing degaussers may not have sufficient force to effectively degauss such media.

Cryptographic Erase (CE) is an emerging sanitization technique that can be used in some situations when data is encrypted as it is stored. With CE, media sanitization is performed by erasing the cryptographic keys that were used to encrypt the stored data, as opposed to sanitizing the storage locations on media containing the encrypted data itself. However, operational use of CE today presents some challenges. In some cases, it may be difficult to verify that CE has effectively sanitized media. SP 800-88 Revision 1 describes this challenge and possible approaches.



Conclusion

Both revolutionary and evolutionary changes make sanitization decisions more challenging, as the storage device may not clearly indicate what type of media is used for data storage. The burden falls on the user to accurately determine the media type and apply the appropriate sanitization procedure. SP 800-88 Revision 1 will assist organizations and system owners in making sanitization decisions. It does not, and cannot, specifically address all known types of media; however, the described sanitization decision process can be applied broadly.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.