August 2006

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

PROTECTING SENSITIVE INFORMATION PROCESSED AND STORED IN INFORMATION TECHNOLOGY (IT) SYSTEMS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Information systems capture, process, and store information using a wide variety of media. Information is recorded on data storage media and on the devices that create, process, or transmit the information. This information must be protected from creation to disposal in a way that is appropriate to the sensitivity and value of the information. When they discard media and devices, organizations and individuals should make sure that proper techniques are used to remove the data, or to destroy the media, to protect the confidentiality of the information.

Media sanitization is the process for removing confidential data from storage media, with reasonable assurance that the data cannot be retrieved and reconstructed. Data that has been improperly or unsuccessfully removed from media could be recreated by attackers or by unauthorized individuals. The sanitization process is especially critical when storage media are transferred, become obsolete, are no longer usable, or are no longer required by an information system. All of the residual magnetic, optical, or electrical representation of data that has been deleted from the media must not be easily recoverable.

NIST Special Publication 800-88, *Guidelines for Media Sanitization*

NIST's Information Technology Laboratory recently issued Special Publication (SP) 800-88, *Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology*, to help organizations securely manage the information processed and stored on devices and media. Authors Matthew Scholl, Richard Kissel, Steven Skolochenko, and Xing Li discuss in detail the decision process concerning media that has been identified for disposal or reuse, and media that is no longer under the effective control of the organization. The guide, used along with local policies and procedures, will enable managers to make effective, risk-based decisions for the effective sanitization of the information recorded on the media and for the disposal of the media. Publication of the guide was supported by the Department of Homeland Security (DHS).

NIST SP 800-88 discusses the basic types of information, the available sanitization methods, and the different types of media, and provides information on techniques for removing data and disposing of media. The guide gives details on the procedures and principles that influence sanitization decisions and includes a decision matrix to aid the decision-making process. The appendices include tables of minimum recommended sanitization techniques for clearing, purging, or destroying various media. These tables can be used with the decision flowchart to identify the needed steps for secure media handling. Also included in the appendices are a glossary of terms, a listing of tools and resources that can assist in decisions about media sanitization, information about media sanitization specifically targeted to home computer users, and a list of references.

The guide can be accessed at http://csrc.nist.gov/publications/nistpubs/index.html.

continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since September 2005:

The Process for Managing Media Sanitization

An important step that federal organizations should take to securely manage their information and media is to categorize their IT systems in accordance with Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. FIPS 199 requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The standard defines these three levels of impact as the potential impact on the organization should there be a breach of security (a loss of confidentiality, integrity, or availability). Based on the results of categorization, organizations should then select appropriate controls to protect their systems and information. The needed controls are discussed in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.

The critical factors affecting information disposition and media sanitization should be determined at the starting phase of system development, when the system security plan is developed. For information about developing security plans, see NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*.

The initial system requirements should include hardware and software specifications as well as interconnections and data flow documents that will assist the system owner in identifying the types of media used in the system. Decisions made at this time affect the resources needed for sanitization for the remainder of the system life cycle.

A determination should be made during the requirements phase of system development about what other types of media will be used to create, capture, or transfer information used by the system. This analysis, balancing business needs and risk to confidentiality, helps the organization determine the media that will be considered for the system. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, assists organizations in the risk-based analysis of security requirements.

Once an organization has completed an assessment of its system confidentiality, determined the need for information sanitization, and determined the types of media used and the media disposition, an effective, risk-based decision can be made on the appropriate and needed level of sanitization.

The organization should document decisions about sanitization of media and ensure that a process and proper resources are in place to support these decisions. Information disposition and sanitization decisions occur throughout the system life cycle. During the life of an information system, many types of media, containing data, will be transferred outside the control of the system. Some media will be reused during all of the stages of the system life cycle. These conditions reflect the changing requirements for media during activities such as system maintenance, upgrades to systems, and configuration updates.

Frequently, the sanitization of media and the disposition of information are carried out during the last phase of the system life cycle. At this phase, decisions about media sanitization should be made before disposal or release of the media for reuse outside the organization, or the media should be destroyed.

Decisions about the proper sanitization methods for information should be based on the level of confidentiality of the information that is placed on the media. The electronic media used in today's IT systems are assumed to contain information that corresponds to the system's security categorization for confidentiality.

Other issues to be considered in decisions about media sanitization include federal agency requirements for the retention of records and for maintenance of records. Agency officials responsible for implementing Privacy Act and, Freedom of Information Act (FOIA) functions should be consulted. Officials responsible for maintaining an agency's historical information should also be consulted. These consultations should be ongoing, as controls may have to be adjusted as the system and its environment change.

Organizations should track, document, and verify media sanitization and destruction actions, and periodically test the sanitization equipment and procedures to ensure correct performance.

NIST SP 800-88 recommends that organizations establish an information security governance structure for its media sanitization decisions. The guide describes the security responsibilities of everyone in the organization—from program managers and agency heads to users.

Media types are expected to change as the technology changes. However, the process for media sanitization should always focus on protecting the information that is recorded on the media.

Who We Are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

Methods for Media Sanitization

After organizations have categorized their information, assessed the nature of the medium on which it is recorded, assessed the risk to confidentiality, and determined their future plans for the media, they can then decide on the appropriate process for sanitization. Factors to be considered in sanitization are cost, environmental impact, and the need to protect the confidentiality of the information.

There are two primary types of media:

* Hard copy media are physical representations of information, such as paper printouts, printer, and facsimile ribbons, drums, and platens. Disposal of these types of media is often uncontrolled, leading to potential significant vulnerabilities if the information is improperly disclosed.

* Electronic media are the bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment, and many other types of electronic equipment.

The methods of media sanitization are:

* Disposal of the media, by discarding the media without any sanitization procedures. Processes include the recycling of paper and other media that do not contain confidential information.

* Clearing the media by deleting information using methods that prevent retrieval by data, disk, or file recovery utilities, and that resist keystroke recovery attempts executed from standard input devices and from data scavenging tools. Overwriting is an acceptable method for clearing media and protecting the confidentiality of the information. Software and hardware products are available to overwrite storage space on the media with nonsensitive data. The logical storage location of a file, such as the file allocation table, as well as all addressable locations can be overwritten, replacing the written data with random data. Overwriting cannot be used for media that are damaged or that are not suitable for overwriting.

* Purging the media to protect the confidentiality of information against a laboratory attack, such as the use of signal processing equipment by specially trained personnel to recover data. Degaussing is a purging method that exposes the magnetic media to a strong magnetic field from a permanent magnet or electromagnetic coil to disrupt the recorded magnetic domains. Degaussing can be an effective method for purging damaged media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. Degaussing cannot be used to purge nonmagnetic media, such as compact disks (CDs) or digital versatile discs (DVDs).

* Destroying the media to prevent its reuse. Destruction techniques include disintegration, incineration, pulverization, and melting of the media. Paper and flexible diskettes that have been removed from their outer containers can be shredded to an appropriate shred size so that the information cannot be reconstructed. Sanding the media by applying an abrasive tool and treating the surface with chemicals can also be used to completely remove the media recording surface. Optical mass storage media, including compact disks (CDs, CD-RW, CD-R, CD-ROM), optical disks (DVDs), and magneto-optic (MO) disks must be destroyed by burning, pulverizing, crosscut shredding, or grinding the information-bearing surface. These processes should be carried out by trained and authorized personnel at an approved facility.

If it is not practical to use the clearing and purging methods, then destruction of the media is recommended. For example, paper media of moderate confidentiality cannot be purged; therefore, the media should be destroyed.

See NIST SP 800-88 for details on all of these methods.

Other Guidance and Standards Supporting the Secure Handling of Information

Some of the NIST publications that support the secure handling of information and media sanitization include:

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, provides guidance for establishing the security categorization for a system's confidentiality. This categorization will impact the level of assurance an organization should require in making sanitization decisions.

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, sets a base of security requirements that enables an organization to have an effective media sanitization program.

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, assists organizations in developing security plans that summarize the security requirements for each information system, and the security controls in place or planned for meeting the requirements.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance to organizations in identifying the risks to their information systems, assessing the risks, and taking steps to reduce the risks to an acceptable level. The risk management process enables organizations to protect the information systems that store, process, and transmit organizational information, to make well-informed risk management decisions, and to apply system authorization and accreditation processes.

NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, provides information on commercial products that can be used for clearing, purging, and destroying media.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, provides information about minimum recommended security controls to protect the confidentiality, integrity, and availability of information systems and information, including the controls for media protection and sanitization. The controls are administrative, operational, and technical safeguards that are selected, based on the system security categorization.

NIST 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, assists organizations in identifying information types and impact levels, and assigning impact levels for confidentiality, integrity, and availability. The impact levels are based on the security categorization definitions in FIPS 199.

These and other NIST publications can help you in planning and implementing a comprehensive approach to IT security. Information about the NIST publications that are referenced in this bulletin, as well as other security-related publications, is available at http://csrc.nist.gov/publications/index.html

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.

ITL Bulletins via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message HELP. To have the bulletin sent to an e-mail address other than the FROM address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.