

GENERAL SERVICES ADMINISTRATION  
Washington, DC 20405

July 8, 1994

FIRMR BULLETIN C-22  
SUPPLEMENT 1

TO: Heads of Federal agencies  
SUBJECT: Security and privacy protection of Federal information  
processing (FIP) resources

1. Purpose. This bulletin provides information and guidance to help agencies achieve security and privacy protection for FIP resources, including those resources provided by contractors.

2. Expiration date. This bulletin contains information of a continuing nature and will remain in effect until canceled.

3. Contents.

Topic	Paragraph
Related material.....	4
Information and assistance.....	5
Definitions.....	6
Acronyms.....	7
Background.....	8
Security program elements.....	9
Identification and review.....	9a
Security controls.....	9b
Continuity of operations.....	9c
Security audits or evaluation.....	9d
Physical and environmental security.....	9e
Contingency plan.....	9f
National security and emergency preparedness.....	9g
Management.....	10
Security administration.....	10a
Security training and awareness.....	10b
Malicious software.....	10c
Disposition of sensitive automated information.....	10d
Acquisition specifications.....	10e
Considerations for contractor-run systems.....	10f
Technology.....	11
Data encryption standard.....	11a
Digital signature standard.....	11b
Electronic certification.....	11c
Electronic data interchange.....	11d
Network access and authentication.....	11e
Trusted systems technology.....	11f

FEDERAL INFORMATION RESOURCES MANAGEMENT REGULATION  
APPENDIX B

FIRMR Bulletin C-22  
Supplement 1

Telecommunications.....12  
Voice.....12a  
Video.....12b  
Private branch exchange.....12c  
Disposition of sensitive automated information...Attachment A

4. Related material.

Computer Security Act of 1987, 40 U.S.C. 759 note.

Privacy Act of 1974, 5 U.S.C. 552a.

OMB Circular A-130, Management of Federal Information Resources.

FIRMR Part 201-18, Planning and Budgeting.

FIRMR Section 201-21.3, Security and Privacy.

FIRMR Bulletin C-20, National Security and Emergency

Preparedness (NSEP) Telecommunications.

FIRMR Bulletin C-28, Computer Viruses.

47 CFR Part 64 - Appendix A.

NIST Publication List 91, Computer Security Publications.

GSA brochure, "Information Resources Security: What Every Federal Manager Should Know".

National Computer Security Center, "A Guide to Understanding Data Remanence in Automated Information Systems" (NCSC-TG-025, Library No. S-236,082, Version-2).

5. Information and assistance.

a. For additional information or assistance concerning the subject matter in this bulletin contact the address below:

General Services Administration

Regulations Analysis Division (KMR)

18th and F Streets, NW.

Washington, DC 20405

Telephone: FTS/Commercial (202) 501-3194 (v) or

FTS/Commercial (202) 501-0657 (tdd)

b. For information or assistance concerning security planning or support using Government and contractor security consultants or services contact the address below:

General Services Administration

Office of Technical Assistance

GSA Federal Systems Integration & Management Center (FEDSIM)

5203 Leesburg Pike, Suite 400

Falls Church, VA 22041

Telephone: FTS/Commercial (703) 756-4111 (v)

FIRMR Bulletin C-22  
Supplement 1

c. For information on assistance concerning regional or local ADP security support provided through commercial contracts contact the GSA, Ofc of Technical Assistance, Federal Information Systems Support Program, 5203 Leesburg Pike, Suite 501, Falls Church, VA, 22041, Telephone FTS/Commercial (703) 756-4227.

6. Definitions. The following definitions apply to this bulletin as follow:

"Risk analysis" means identification of the events, threats, or hazards that could have an adverse impact on FIP resources and an understanding of the impact of loss or compromise of information on the organization, expressed in economic or social terms, and the probability of such a loss occurring.

"Sensitive information" means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

"Trusted systems technology" means the technical methods and mechanisms used to develop computer systems which employ adequate hardware and software measures that allow simultaneous processing on a range of sensitive or classified information.

7. Acronyms.

ANSI American National Standards Institute  
DES Data Encryption Standard  
DSA Digital Signature Algorithm  
DSS Digital Signature Standard  
EDI Electronic Data Interchange  
EFT Electronic Funds Transfer  
EPL Evaluated Products List  
FIP Federal Information Processing  
FIPS Federal Information Processing Standard  
MAC Message Authentication Code  
NIST National Institute of Standards and Technology  
NSA National Security Agency  
NSEP National Security and Emergency Preparedness  
OMB Office of Management and Budget  
PBX Private Branch Exchange  
PIN Personal Identification Number  
SOW Statement of Work  
TSP Telecommunications Service Priority System

FIRMR Bulletin C-22  
Supplement 1

8. Background.

a. FIRMR Part 201-18 requires agencies to consider security and privacy needs in the development of their five year plan for meeting the agency's information technology needs.

b. FIRMR Subpart 201-21.3 requires each agency to ensure that:

(1) A proper level of security is maintained for all FIP resources, including those maintained or provided by contractors, or state or local governments;

(2) FIP resources are operated and maintained to safeguard the confidentiality, integrity, and availability of information, including prevention of loss from natural hazards, fire, and accidents; and

(3) FIP resources are operated and maintained in a manner that protects the personal privacy of individuals; and

(4) Operations are continually reviewed to ensure that security and privacy safeguards are implemented, operated, and monitored in accordance with approved security and privacy policy guidance documents.

c. This bulletin advises Federal managers about computer security and privacy considerations and technologies. It is not the intent of this bulletin to provide an exhaustive treatment of every aspect of information security. NIST Publication List 91 contains publications that provide specifics on these topics. This bulletin provides an overview of contemporary computer security and privacy issues. The bulletin discusses three general categories of security: management, technology, and telecommunications.

9. Security program elements. Agency security and privacy programs should include the following procedures and safeguards:

a. Identification and review. For each FIP system, the agency should determine the level of security required and perform a risk analysis to provide an understanding of the probable losses and the effect of those losses upon the agency mission. The review of each system should determine that only information essential to the system's purpose is maintained. The Privacy Act of 1974 requires that agencies maintain only that information about an individual which is relevant and necessary as required by statute or executive order of the President.

FIRMR Bulletin C-22  
Supplement 1

Thus, one way of protection of privacy is promoted by agencies limiting the amount of information maintained to accomplish a purpose of the agency.

b. Security controls. Administrative, physical, and technical controls help meet agency security program objectives. Examples include--

(1) Controls that have the potential to reduce damage or loss to the agency through concentration or distribution of FIP resources functions;

(2) Controls used to protect data during physical handling;

(3) Controls that identify and ensure the accountability of individuals whenever an action is taken that may have an effect on the data, application, or physical installation; and

(4) Controls that limit or prevent access to FIP resources and that record entry attempts.

c. Continuity of operations. To ensure continuity of operations during an emergency or situations when the primary FIP systems support is interrupted, agencies should--

(1) Identify critical computer records and develop a contingency plan for each FIP system that processes sensitive information;

(2) Identify essential programs, systems of records, and alternative sites or services;

(3) Develop an agreement to use and periodically operate at an alternate facility or service center;

(4) Duplicate essential information, programs, and documentation for backup at an off-site protected location; and

(5) Assure that all sites meet current fire codes and regulations. Have the fire department inspect the site and test fire protection systems and safeguards.

d. Security audits or evaluation.

(1) Agencies should perform audits to evaluate the adequacy of security safeguards, including FIP systems operated by contractors.

FIRMR Bulletin C-22  
Supplement 1

(2) Audits should be conducted by personnel other than those responsible for operating and developing the system.

(3) The audit or evaluation should include an examination of information sensitivity; a verification and validation of the adequacy of physical, administrative, and technical controls; and a review of the adequacy of security administration. The agency should determine time intervals for audits or evaluations on the basis of the sensitivity of the operation, but should conduct one at least every three years. This audit should ensure that all applicable Federal policies, regulations, and standards are met and that logs and inventories are current.

e. Physical and environmental security. Agencies should maintain a safe physical environment for FIP resources that ensures the protection of personnel, the safeguarding of the physical assets of the facility, and the effective accomplishment of the facility's mission. Ventilation, smoke detection, fire, flooding, emergency power, and personnel safety are major factors to consider when developing environmental security safeguards.

f. Contingency plan. Agencies should develop, test, and maintain a contingency plan for each FIP system that processes sensitive information in the event of an emergency or crisis where the primary FIP system becomes unavailable (e.g., fire, flood, earthquake) and disaster recovery is necessary.

g. National security and emergency preparedness (NSEP). Certain telecommunications resources are installed and operated to meet agency NSEP requirements. Agencies need to identify resources that use telecommunications services and transmit sensitive information. These FIP resources should be considered for, and application made for TSP Authorization Code assignment under the TSP system, if these services qualify as NSEP. The TSP System was implemented on September 10, 1990, and replaced the former Restoration Priority (RP) System. FIRMR Bulletin C-20 contains guidance on NSEP. See Appendix A to 47 CFR Part 64 for TSP system coverage.

10. Management. Some aspects of security are simply good management. No matter how many technical controls are in place, there is no substitute for careful management of personnel, procedures, and controls. Rules must be set for employees and they must understand and take responsibility for security. Accordingly, effective management of an information security program requires a written information security policy, sound personnel hiring practices, training and awareness programs,

FIRMR Bulletin C-22  
Supplement 1

periodic risk analysis, periodic review and certification, and contingency planning. These fundamental security management requirements are clearly stated in OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems. A published agency information security policy disseminated to all subordinate levels to implement clearly sends a message that senior management supports the organization's information security program. The conduct of a periodic risk analysis will identify weaknesses in safeguards that require added security controls, and concurrent contingency planning will ensure continuous processing capability for applications that support the business of the organization. Other important considerations in security management follow.

a. Security administration.

(1) Security administration involves activities that not only protect the system from unauthorized disclosure and modification but ensure the system remains available for agency use. Details on how to administer system-specific controls are not addressed in this bulletin, but NIST Publication List 91 contains sources for this information. There are, however, general security administrative functions that apply to all systems. These include:

- (i) Publicizing the security policy within the agency.
- (ii) Establishing and maintaining system logon and access controls (passwords).
- (iii) Performing risk analyses.
- (iv) Training users.
- (v) Conducting periodic audits of system safeguards and procedures.
- (vi) Developing contingency plans.

(2) Administering security involves tradeoffs. When evaluating the organization's most important information assets and how they may be protected, consider protective measures that yield appropriate security at reasonable costs. Keep in mind that to have an effective computer security program, all components must function together and in reasonable harmony to achieve success.

FIRMR Bulletin C-22  
Supplement 1

b. Security training and awareness.

(1) Training is a major component of a successful automated information protection program since security infractions may be the result of human actions that stem from inattention and unawareness of security issues. Developing security awareness among the staff can result in prevention and early detection of problems and losses. Target audiences for technical and awareness training include executives and policy makers, program and functional managers, security and audit personnel, computer management operations and programming staff, and end users.

(2) Training should be accomplished in the context of organizational policies and procedures using training resources such as written materials, presentations and classes, audiovisual and computer-based courses. The training provided should create an awareness of the risks to automated information systems security and privacy, and the importance of safeguards. Agency personnel should be informed about the FIP system environment they use, types of security and privacy data maintained, and penalties imposed for violation or disregard of agency security policies, procedures, and controls. When possible training should emphasize specific responsibilities of the individuals being trained.

c. Malicious software.

(1) Computer viruses and related malicious software attacks have become a significant problem undermining the effective and confident use of computer technology in Government and industry. Viruses can spread from program to program within systems and from systems to systems without limit. Sometimes users and administrators of shared systems do not take adequate precautions to ensure the quality and safety of the systems and software they are using.

(2) Careful acquisition and use of computer software and prudent administration of security controls and procedures is an excellent defense against harm to computer systems. Anti-viral software is another valuable asset which should be employed to verify whether it is safe to use or distribute software. Agencies should implement the use of anti-viral software within their computer systems environment to reduce the vulnerability of damage to computer resources. There are three types of anti-viral software:

(i) Preventive--places barriers (i.e., access control, encryption) in the path of program modification.

FIRMR Bulletin C-22  
Supplement 1

(ii) Detective--monitors events in a computer and reports suspect ones to user.

(iii) Scanning--tests for the attributes of known viruses.

(3) The growing use of portable computers, the surge of local area and wide area networks, and expanded use of electronic transfer of data have increased the complexity of virus protection. Evolving technology has expanded the tasks and responsibilities to keep computer systems virus free. Educating users, emphasizing their responsibilities, and helping them apply good judgment where computer security is concerned will offer better security and integrity to Federal information systems.

d. Disposition of sensitive automated information.

(1) Agencies must establish internal procedures which ensure the proper disposition of sensitive automated information. Sensitive information must always be protected from unauthorized access and disclosure. An aspect of safeguarding and controlling sensitive information that is often overlooked is that of data "residue" left on disk or in memory. When a file is "erased" or "deleted" the data does not completely disappear. It remains on the computer's hard disk drive, floppy disk, or in memory until it is overwritten. It is a simple matter to "restore" a file, and in fact there are many software utility programs designed for just this purpose. Consequently, agencies must take action to ensure all sensitive information is completely removed when its use is no longer required. For these reasons, it is important to sanitize or "wipe clean" from disks sensitive information before releasing the storage area for reuse.

(2) To accomplish this objective, memory should be overwritten using appropriate application software and the overwrite should be verified. The number of times information is overwritten depends upon its level of sensitivity. In any case, overwriting information using 0's should be performed at least once. Software is available that will overwrite sensitive information. Approved degausser equipment may also be used to sanitize information from disk storage. The National Computer Security Center has developed "A Guide to Understanding Data Remanence in Automated Information Systems" (NCSC-TG-025) which discusses clearing and purging national security classified data from storage media. This publication may be helpful to agencies responsible for the secure handling of sensitive or classified FIP system memory and secondary storage media. Attachment A provides additional information on the disposition of sensitive automated information.

FIRMR Bulletin C-22  
Supplement 1

(3) Additionally, every precaution should be taken to remove duplicate versions of sensitive files. Be aware that even when sensitive information has been eradicated from a disk, there are other places where this information may still reside.

Examples include the following:

(i) The data may have been copied onto the same or different storage media.

(ii) Backup copies may have been created by other application software. For example, word processing software may automatically create backup copies that duplicate sensitive data.

(iii) User application software may have created temporary files containing sensitive information that has not been removed.

(iv) Earlier versions of information may have been reassigned to other areas in unallocated clusters.

(v) Information data files (residue) may reside in hidden files or extended memory after exiting.

(4) Users should find and remove all traces of data from the storage media when the sensitive information is no longer needed. Users and responsible officials should also remember that the FIP equipment used to process sensitive information may: require maintenance or repair, be transferred or loaned, be declared surplus or excess and disposed of, be used by others who should not have access, or be shipped by mail or commercial carrier for some reason. Whenever any of these or similar conditions occur, the sensitive information or components must always be completely protected or permanently deleted from the FIP equipment.

e. Acquisition specifications.

(1) Properly integrating security controls is essential to a workable and cost-effective security program. It is important, therefore, that agencies identify and include requirements in specifications for security and privacy controls and related security services. By doing so, greater assurance is provided that an array of security controls have been considered and are mutually supportive of each other. If security and privacy is built in at the inception, in the acquisition phase, agencies will achieve better security and find it easier and less expensive over the long term process. The period in which

## FIRMR Bulletin C-22

security controls are incorporated is not as important as ensuring that security requirements have been considered. NIST Special Publication 800-4, "Computer Security Considerations in Federal Procurements", provides information that will help agencies identify system security requirements.

(2) There are circumstances when an agency can benefit from employing contractor computer security services. Time, budget, availability, and skill are factors that weigh in this decision. When contracts are used, clear and concise specifications must be included in solicitations for computer security and privacy services. The contractor will then use these specifications to effectively perform security activities for the agency. A NIST Publication, NISTIR 4749, "Sample Statements of Work (SOW) for Federal Computer Security Services," provides sample statements of work for frequently performed computer security activities. These SOW's are intended to promote consistent and high quality computer security services.

f. Considerations for contractor-run systems.

(1) The Computer Security Act of 1987, OMB Circular A-130, and various FIPS publications clearly establish that agencies are responsible for ensuring that adequate security is maintained at installations operated by or on behalf of the Federal Government. It is important, therefore, that each Federal agency communicate computer security and privacy requirements to contractors or other organizations, including state and local governments, and other entities which may be acting on behalf of a Federal agency. Both the system owner and contractor are responsible for assuring that adequate protections are in place to meet contract specifications and also that contractor personnel receive computer security awareness training.

(2) Contractors operating on behalf of Federal agencies are bound by the same laws and regulations that govern the agencies. OMB Circular A-130 requires that, "...contractor personnel involved in the management, operation, programming, maintenance, or use of information technology be aware of their security responsibilities and know how to fulfill them."

11. Technology. A large market exists for secure products that are low-cost and easy to use. The following describes several technical security controls.

## FIRMR Bulletin C-22

a. Data encryption standard. FIPS 46-1, Data Encryption Standard (DES), is for use in protecting the confidentiality and integrity of unclassified data in Federal computer systems when the agency determines that cryptographic protection is required. Applications of DES include privacy protection of personal information, message authentication, personal authentication, password protection and access control.

(1) DES consists of two parts: an algorithm and a key. The algorithm is a complex, iterative process that converts plaintext to ciphertext using a 56-bit key (a very long string of numbers). The goal is to completely scramble the data so it has the appearance of random, unintelligible data, called ciphertext. The same key can transform the ciphertext back to plaintext, a process called decryption.

(2) Heads of Federal agencies may waive the use of DES when compliance with the standard would adversely affect the organization's mission or cause major adverse financial difficulty. Section 17 of FIPS 46-1 details the procedures for approving waivers.

b. Digital signature standard. DSS, which is currently in draft, prescribes the Digital Signature Algorithm (DSA) which can be used to generate a digital signature. DSA authenticates the integrity of the signed data and the identity of the signer. DSA may also be used in proving to a third party that data was signed by the generator of the signature.

(1) DSS will be applicable to all Federal agencies for the protection of unclassified information that is not subject to section 2315 of Title 10, United States Code, or section 3502(2) of Title 44, United States Code. These Codes apply to national defense and intelligence activities. When approved as a FIPS, DSS will be used in designing and implementing public-key based signature systems for Federal departments and agencies.

(2) DSA is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications which require data integrity assurance and data origin authentication. DSA may be implemented in software, firmware, or hardware.

c. Electronic certification. Many Federal Government agencies are transforming paper-based systems into electronic systems. This approach has proven that it reduces costs and increases productivity. In paper-based systems, the written signature is used to bind the signer to the terms of the document

## FIRMR Bulletin C-22

being signed. Electronic certification has been developed as an electronic replacement of the written signature. Like the hand-written signature, electronic certification identifies the person responsible for the electronic document. Electronic certification can also be used to verify that the document has not been altered after it was electronically certified.

(1) Electronic certification is accomplished using either secret key cryptography or public key cryptography. Secret key cryptography, such as DES, is based on the use of a cryptographic key shared between two parties. When using secret key cryptography to electronically certify a document, a cryptographic checksum is calculated using DES. This checksum is known as a MAC and is defined in FIPS Publication 113. NIST validates all products to ensure they are in conformance with FIPS Publication 113.

(2) Public key cryptography uses two keys: a private key that is known only to its owner and a public key which is publicly available. Using the private key, documents are electronically signed by generating an electronic signature. The signature and document are usually stored or transmitted together to the verifier who verifies the signature using the public key of the signer.

d. Electronic data interchange. EDI is the computer-to-computer interchange of messages representing business documents. EDI promises to provide a significant improvement in the quality and efficiency of these business interactions. FIPS 161, Electronic Data Interchange, adopts for Federal government use voluntary industry standards for formatting and transmitting electronic messages between data interchange partners. A paperless process called "electronic commerce" is evolving and will integrate EDI and other electronic techniques to exchange information between government agencies and external organizations to accomplish business transactions. Consideration, however, must be given to the security issues inherent in the use of computers and telecommunications to accomplish traditional paper-based functions. Specific activities must be undertaken to ensure that EDI messages are authentic, properly authorized, and are completely and accurately retained with audit trails for accountability. Additionally, EDI messages must be protected from loss, modification or unauthorized disclosure during communication and storage.

(1) Two security standards have been developed by the Accredited Standards Committee (ASC) X12 (EDI) for use in the EDI environment. ANSI X12.58 (Security Structure) uses ANSI X9.9 (Financial Institution Message Authentication (Wholesale)) and

X9.23 (Financial Institution Encryption of Wholesale Financial Messages) as models for message authentication and encryption for the EDI environment.

(2) Message authentication, as addressed in ANSI X9.9, allows the ability to prove the source of a message to the receiver as well as provide an assurance that the message has not been modified. Encryption provides privacy for a message. Both message authentication and encryption are provided by using the DES algorithm and a secret cryptographic key. ANSI X12.42 (Cryptographic Service Message) specifies a transaction set format for transferring ANSI X9.17 (Financial Institution Key Management (Wholesale)) key management messages and distributing secret keys to data interchange partners.

(3) X12 is developing a guideline for implementing ANSI X12.42 and X12.58. The guideline contains detailed information for implementors describing the options within ANSI X9.9, X9.23 and X9.17 and why each might be selected for use in a particular application. Examples of messages using the security provided by these standards are also provided.

(4) Work has also been initiated to provide a non-repudiation capability using public key techniques. Non-repudiation is the ability to prove the source of a message to both the receiver and a third party. Work has also been initiated to provide a non-repudiation capability using both secret key and public key techniques. This authenticity capability will provide proof of the source of a message to both the receivers of that message and a third party.

e. Network access and authentication. The proliferation of networked computer systems has made it possible to access many computers from a terminal located almost anywhere in the world. As a result, it has become critical to ensure the security of the access control process for these networked computer systems. Increased access control is particularly important for those systems dealing with sensitive information and mission critical operations.

(1) The ability to verify the identity of individual computer users is a primary requirement for effective access control systems. If users cannot be identified with some degree of accuracy, it becomes impossible to protect the computer resources accessed by those users. Traditionally, computer users have been required to memorize "secret" passwords and then present these passwords when requesting access to the system. Authentication based only on passwords can be effective, but this must be closely managed and monitored.

## FIRMR Bulletin C-22

(2) Advances in authentication technology have provided a number of practical alternatives to password-only authentication. There are three generally accepted methods for verifying the identity of a user. These routines include:

- (i) Something the user knows, such as a password;
- (ii) Something the user possesses, such as an authentication token; and,
- (iii) Some unique physical characteristic of the user.

(3) Token-based authentication schemes require the user to produce a physical token which the system can recognize as belonging to that particular user. A familiar example of this type of system is the automatic teller machine, which identifies users by a magnetically coded plastic card in combination with a personal identification number (PIN). More sophisticated systems often use a token that contains a microprocessor and semiconductor memory. These devices are capable of storing cryptographic keys and performing security cryptographic authentication protocols.

(4) Biometric authentication systems verify the identity of system users by recognizing a physical characteristic such as a fingerprint, voice pattern, or retinal pattern. When a user attempts to access the system, a current pattern is obtained and compared to the enrollment template for the user. If the template matches the current pattern, the user is granted access.

(5) Although tokens and biometrics can improve the security of access control systems when used individually, security can be further strengthened and improved by using a combination of methods. In many cases, particularly those involving high levels of security, the most effective approach is to use some combination of tokens, biometrics, and passwords for more positive authentication.

(6) NIST Computer Systems Laboratory Bulletin, Advanced Authentication Techniques, November 1991, provides information on evaluating, procuring and integrating user authentication systems. Some of the factors to be considered are cost, performance, accuracy, reliability, maintainability, commercial availability, and interoperability.

f. Trusted systems technology. There is no binding national policy on the use of trusted systems technology in Federal computer systems which process unclassified information. NIST recommends the use of trusted technology when it satisfies requirements for adequate and cost-effective access control protection.

(1) Agencies with a need for systems with trust technology features, based on a formal risk management procedure, should select these systems from the NSA evaluated products list (EPL). If EPL products are not available, then agencies may select or design systems that best meet their security requirements using the "U. S. Department of Defense Trusted Computer System Evaluation Criteria" (DOD 5200.28-STD) publication, often referred to as the "Orange Book."

(2) NIST and NSA are developing standards and guidance on trust technology to help Federal agencies determine the full set of protection mechanisms that may be effectively applied to computer systems. As new technology evolves NIST and NSA will continue to keep Federal agencies informed on this subject.

12. Telecommunications. Currently, cryptography is the primary means for protecting telecommunications systems. Examples of telecommunications components where cryptography is incorporated include: secure telephones, secure mobile radio, secure cellular telephones, secure integrated services digital network (ISDN), secure facsimile, secure data transmission, and secure signature. Some of these communications technologies are discussed here.

a. Voice. Privacy and security in voice telephone conversations may be compromised by direct wiretaps, interception of terrestrial or satellite microwave links, crosstalk in the network, or listening by an intruder on an extension or party line. Cellular and cordless telephones are particularly vulnerable since the broadcast radio signals they use are easily intercepted.

(1) Wiretapping and interception of cellular telephone signals are generally illegal. This protection does not extend to ordinary cordless telephones, however. In fact, incidents where conversations are overheard are common since only ten frequency channels are allocated to these devices. Many cordless units now include a password system to protect against fraudulent outgoing calls by another party.

FIRMR Bulletin C-22  
Supplement 1

(2) The Secure Telephone Unit-3 (STU-3) telephones provide cryptographic protection for voice, data, and facsimile telephone communications. The GSA Information Security Management Division provides a spectrum of security services for the protection of voice and data. Information may be obtained from this office by calling (202) 708-7310.

b. Video. Unauthorized interceptions of satellite and cable analog video signals are a significant problem today. "Scrambling" of these signals is widely used to deter video piracy. However, scramblers do not provide adequate security for sensitive video communications because strong cryptography is not used, and decoders are available to unauthorized users. Additionally, microwave video signals are more easily intercepted than coaxial cable signals. While fiber optic cables are least vulnerable to intrusion, signals can be intercepted nonetheless. Cryptographic devices can provide protection for digital channels such as DS-3 and DS-1 and may be used to protect video signals when they are carried over these channels.

c. Private branch exchanges. PBX's are vulnerable to attacks that may result in denial of service, compromises of confidentiality, and frequently, fraudulent use of telephone services. Attacks may come from "insiders" who abuse legitimate knowledge of the specific configuration and features of the PBX, or from "outsiders" who have only a general knowledge. Management controls of access to switching equipment, passwords, and other sensitive information protect against insider attacks. Remote maintenance and management features may provide opportunity for intrusion. PBX vendors offer a variety of features and options intended to limit remote access and to deter and detect security compromises. Agencies should consider the specific security features offered when procuring PBXs. Routine and timely audits of logs and billing information may reveal an attack in time to limit the damage and to facilitate identification of the perpetrator.

JOE M. THOMPSON  
Commissioner  
Information Resources  
Management Service

FIRMR Bulletin C-22  
Supplement 1  
Attachment A

DISPOSITION OF SENSITIVE AUTOMATED INFORMATION

1. Background.

a. This attachment provides additional information to that in paragraph 10 d. of this bulletin regarding the disposition of sensitive (unclassified or classified) automated information. It incorporates information published in the NIST and National Computer Security Center (NCSC) advisory material concerning the sensitivity of automated information and methods of disposing of sensitive automated information (See references in paragraph 6).

b. Sensitive automated information must be completely removed from any electronic or magnetic storage media (such as magnetic tape, magnetic disk, optical disk) on which it is stored so that the information cannot be retrieved. Occasionally, Federal agencies have transferred, released, or disposed of FIP equipment without taking appropriate measures to completely remove sensitive data or information which was stored on the system's media. Users may also share information or media, such as diskettes, on which sensitive information is also resident. Others may dispose of diskettes believing that "erasing" the files has destroyed the information on them.

c. Instances such as these can lead to the unintended disclosure of sensitive information, ranging from the less threatening (e.g., individuals' social security numbers) to the life-threatening (e.g., disclosure of controlled intelligence information such as names of Federal undercover agents). The implementation of appropriate disposition procedures to ensure sensitive automated information is completely removed from computer equipment and storage media when it is no longer required will alleviate this problem.

2. Agency security policy and procedures.

a. Federal agencies should establish internal security policies and procedures to ensure the proper disposition of sensitive automated information. The policy should include such things as when unauthorized access to magnetic media is most likely to occur and which data is most at risk; whether contractors who use agency computer systems are aware of agency disposal and sanitization policies; and the procedures used to sanitize leased equipment being returned to the vendor. Agencies should take a risk assessment (analysis and management) approach to protecting information by analyzing both (1) what harm may result if the information is inadequately protected, and (2) the cost of implementing available protective measures.

FIRMR Bulletin C-22  
Supplement 1  
Attachment A

b. Agency policies should include guidance concerning "data remanence," which is the residual physical representation of data that can remain on storage media even after the magnetic or sensitive automated electronic data has in some way been erased or overwritten. This residual information may allow data to be reconstructed, typically using laborious, time-consuming methods. Procedures must also be established and used to check, verify and ensure that all sensitive automated information was completely removed from the storage media and the procedure was effective so there is no data remanence of sensitive automated information.

3. Techniques to remove sensitive automated information from storage media.

a. Three techniques commonly used for removing, clearing, erasing, purging or sanitizing automated sensitive information from storage media are: overwriting, degaussing, and destruction. Degaussing and destruction are the methods normally recommended and preferred above overwriting for the disposition of highly sensitive automated information.

b. As its name implies, overwriting utilizes a program to write (1s, 0s, or a combination of both or even another pattern) onto the location of the media where the file to be sanitized is located. Procedures for the number of times that media is overwritten depends on the level of sensitivity of the information. Users should employ more sophisticated techniques and procedures for highly sensitive data.

c. Degaussing is a method to magnetically erase data from magnetic storage media. The degaussing process involves using an alternating current (AC) to generate a magnetic field to demagnetize magnetic storage media. Two types of degaussers exist: permanent magnet and electric AC degaussers. Degaussers are tested by the Department of Defense. Those which meet their requirements (for use at various security levels of data erasure) and are approved by the National Security Agency (NSA) are placed on the Degausser Products List (DPL), a portion of the NSA's Information Systems Security Products and Services Catalog. Personnel who need to obtain and use such degaussers should consult the DPL and, if necessary, the agency information systems security management office for assistance in this procedure.

d. Destruction of the media containing sensitive automated information may involve incineration, application of an acid solution, or processing at an approved metal destruction facility. Sensitive information should be removed from the media

FIRMR Bulletin C-22  
Supplement 1  
Attachment A

before submitting it for destruction. Most destruction methods or procedures involve potentially hazardous conditions and should be done only by qualified and approved personnel. The NSA NCSC-TG-025 Guide provides specifics on this method and its applicability.

e. The NSA NCSC-TG-025 Guide is a comprehensive document dealing with the secure handling of sensitive or classified information. It provides additional disposition alternatives that may be appropriate depending upon the sensitivity of the data involved. The appropriate agency security office should be consulted for specific guidance, whenever circumstances dictate that complete removal of sensitive automated information is required.

4. Agency and employee security training.

a. Most employees who utilize FIP systems also use, and in fact are often the custodians of, magnetic media. It is therefore important for agencies to give appropriate attention to this subject in the agency computer security training and awareness program. Agency employees should be trained on what constitutes "sensitive information" (i.e. privacy act, medical records, proprietary, etc.) and the risks associated to its disclosure if the information is not removed from the FIP equipment and media. Employee training should include retention properties of FIP equipment and removal procedures for sensitive information (to include verifying complete data removal).

b. Managers, custodians, and users should be informed that media containing sensitive information should not be released without appropriate sanitization. They should coordinate with the necessary records management, security, technical support personnel, and property management personnel who reassign or dispose of the FIP equipment. When data is completely removed from storage media, every precaution should also be taken to remove duplicate versions that may exist on the same or other storage media, back-up files, temporary files, hidden files, or in extended memory.

c. The agency security training and awareness program should include personnel training in technical techniques to check, verify and determine that procedures to remove data remanence for all sensitive automated information were effective; and that all sensitive files were removed. Responsible agency employees must know how to ensure all sensitive automated data is completely removed for situations that require this action, this is especially critical for high sensitivity or high risk areas.

FIRMR Bulletin C-22  
Supplement 1  
Attachment A

5. Disposition of sensitive automated information on other storage technologies. While this Attachment focuses on the need for proper control, disposition, and removal of sensitive automated information from magnetic media, users should be aware that other storage technologies are available (e.g., optical media, electrically erasable programmable read only memory (EEPROM), magnetic bubble memory, and erasable programmable read only memory (EPROM)). Each one may require special disposition procedures for the complete removal of sensitive automated information. Agency records management and security officials should be consulted when these or similar storage media issues arise.

6. References pertaining to this Attachment.

a. NIST Computer Systems Laboratory (CSL) Bulletin, Disposition of Sensitive Automated Information, October 1992. Available by mail from the National Institute of Standards and Technology, B151, Technology Bldg., Gaithersburg, MD 20899. You may also telephone (301) 975-2821 to request a copy of this free publication.

b. National Computer Security Center (NCSC), NCSC-TG-025, A Guide to Understanding Data Remanence in Automated Information Systems, Version 2, September 1991. Available by mail from the National Security Agency, ATTN: IAOC/X811, Ft. Meade, MD 20755-6000. You may also telephone (410) 766-8729 to request a complimentary copy of this publication.

c. NSA's Information Systems Security Products and Services Catalogue (Degausser Products List), updated quarterly by the National Security Agency, Fort Meade, MD 20755-6000. This catalogue may be purchased from the Superintendent of Documents, U.S. Government Printing Office (GPO), Post Office Box 371954, Pittsburgh, PA 15250-7954, as 908-027-00000-1. Cost is \$55 for a yearly subscription which includes quarterly updates of a basic manual in January and July and a supplement in April and October. You may also telephone (202) 783-3238 to order and obtain this publication.

d. NBS Special Publication 500-101, Computer Science and Technology, Care and Handling of Computer Magnetic Storage Media, June 1983. A general guide to preservation of data on storage media particularly magnetic tapes and flexible disk cartridges. This publication may be purchased from the National Technical Information Service, Springfield, VA 22161, as PB83-237271. Cost is \$27 for a paper copy or \$9 for a microfiche. You may also telephone (703) 487-4650 to obtain this publication.

