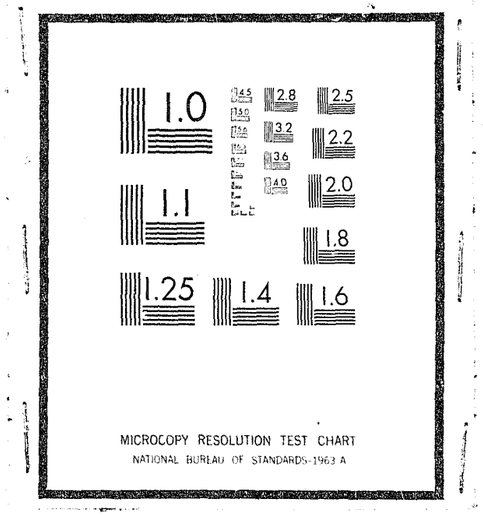

FIPS PUB 39

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

1976 FEBRUARY 15

U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards

GLOSSARY FOR COMPUTER SYSTEMS SECURITY

CATEGORY: ADP OPERATIONS
SUBCATEGORY: COMPUTER SECURITY

U. S. DEPARTMENT OF COMMERCE, Rogers C. B. Morton, *Secretary*
James A. Baker, III, *Under Secretary*
Dr. Betsy Ancker-Johnson, *Assistant Secretary for Science and Technology*

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Acting Director*

Foreword

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official publication relating to standards adopted and promulgated under the provisions of Public Law 89-306 (Brooks Bill) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automatic data processing systems in the Federal Government. To carry out the Secretary's responsibilities, the NBS, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance, and coordination of government efforts in the development of technical guidelines and standards in these areas.

The subject areas of computer security and data confidentiality are of the greatest national interest. The importance of a common vocabulary within these subject areas was recognized by the National Bureau of Standards and was given the highest priority by the Federal Information Processing Standards Task Group on Computer Systems Security. NBS is pleased to make this Glossary for Computer Systems Security available for use by Federal agencies as suggested definitions or interpretations of terms which are relevant in this area.

RUTH M. DAVIS, *Director*
Institute for Computer Sciences and Technology

Abstract

This glossary provides an alphabetic listing of approximately 170 terms and definitions pertaining to privacy, and security related to data, information systems hardware and software. Multiple word terms are listed in natural order, synonyms are referenced, and glossary terms appearing within a definition are indicated.

Keywords: Computer; data processing; definitions; Federal Information Processing Standards Publication; information processing; privacy; security; terms; vocabulary.

Nat. Bur. Stand. (U.S.), Fed. Info. Process. Stand. Publ. (FIPS PUB) 39, 19 pages, (1976) CODEN: FIPPAT

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.
(Order by SD Catalog Number C13.52:39). GPO price 60 cents.
Stock Number 003-003-01576-8

Federal Information Processing Standards Publication 39

1976 February 15

ANNOUNCING THE

GLOSSARY FOR COMPUTER SYSTEMS SECURITY

Federal Information Processing Standards Publications are issued by the National Bureau of Standards pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of Title 15 CFR (Code of Federal Regulations).

Name of Guideline: Glossary for Computer Systems Security.

Category of Guideline: ADP Operations, Computer Security.

Explanation. This Glossary has been prepared in response to the need of Government agencies for a vocabulary of terminology related to the concepts of privacy and computer systems security. The terms have been extracted from many sources and the definitions have been refined through the efforts of the Federal Information Processing Standards (FIPS) Task Group 15—Computer Systems Security. This Task Group was established by the Department of Commerce within the National Bureau of Standards to develop standards and guidelines relative to computer systems security.

Approving Authority. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Maintenance Agency. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Cross Index. See appendix.

Applicability. This Glossary is intended as a reference document to be used throughout the Federal Government to promote common understanding of concepts and procedures relating to computer systems security. It is to be recognized that many terms and definitions in this glossary are highly specialized, and that some terms do have different meanings in other contexts. Other appropriate dictionaries, vocabularies, and glossaries should therefore be consulted in conjunction with use of this glossary.

Implementation. This Glossary is to be regarded as a basic reference document for general use throughout the Federal Government to help promote a common understanding of terminology and concepts relative to privacy and computer systems security. Its use is encouraged but is not mandatory.

Specifications. Federal Information Processing Standard 39 (FIPS 39), Glossary for Computer Systems Security (affixed).

Enhancements. As more experience is gained through the use of this Glossary and through the implementation and research in the fields of privacy and computer systems security, additional terms will be needed and clarifications made.

Suggestions concerning improvements to this Glossary are solicited and should be forwarded to the Associate Director for ADP Standards, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. 20234.

Special Information:

FIPS PUB 11 establishes the American National Standard Vocabulary for Information Processing (X3.12-1970) as a common reference within the Federal Government for terms and definitions used in information processing activities. Items that appear in the X3.12-1970 vocabulary are not included in this glossary of computer systems security terms unless there is a special meaning assigned. Accordingly, this Glossary should be used in conjunction with FIPS PUB 11 and X3.12-1970 and other general dictionaries as appropriate.

Where to Obtain Copies of this Guideline:

a. Copies of this publication are available from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402 (SD Catalog Number C13.5:39). There is a 25 percent discount on quantities of 100 or more. When ordering, specify document number, title, and SD Catalog Number. Payment may be made by check, money order, coupons, or deposit account.

b. Microfiche of this publication is available from the National Technical Information Service, U.S. Department of Commerce, Springfield, Virginia 22151. When ordering refer to Report Number NBS-FIPS-PUB-39 and title. Payment may be made by check, money order or deposit account.

Federal Information Processing Standards Publication 39

1976 February 15

SPECIFICATIONS OF THE

GLOSSARY FOR COMPUTER SYSTEMS SECURITY

access

The ability and the means necessary to approach, to store or retrieve data, to communicate with, or to make use of any *resource* of an ADP system.

access category

One of the classes to which a user, a program or a process in an ADP system may be assigned on the basis of the *resources* or groups of resources that each user, program, or process is authorized to use.

access control

The process of limiting *access* to the *resources* of an ADP system only to authorized users, programs, processes, or other ADP systems (in computer networks). Synonymous with controlled access, controlled accessibility.

access control mechanisms

Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized *access* and to permit authorized access to an ADP system.

access list

A catalogue of users, programs, or processes and the specifications of *access categories* to which each is assigned.

access period

A segment of time, generally expressed on a daily or weekly basis, during which *access* rights prevail.

access type

The nature of an *access* right to a particular device, program or file: for example, read, write, execute, append, modify, delete, create.

accountability

The quality or state which enables violations or attempted violations of *ADP system security* to be traced to individuals who may then be held responsible.

accreditation

The authorization and approval, granted to an ADP system or network to process sensitive data in an operational environment, and made on the basis of a *certification by designated tech-*

nical personnel of the extent to which design and implementation of the system meet pre-specified technical requirements for achieving adequate *data security*.

active wiretapping

The attaching of an unauthorized device, such as a computer terminal, to a communications circuit for the purpose of obtaining *access* to data through the generation of false messages or control signals, or by altering the communications of legitimate users.

add-on security

The retrofitting of protection mechanisms, implemented by hardware or software, after the ADP system has become operational.

administrative security

The management constraints, operational procedures, *accountability* procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data. Synonymous with procedural security.

ADP system security

All of the technological safeguards and managerial procedures established and applied to computer hardware, software, and data in order to ensure the protection of organizational assets and individual privacy.

analysis

See *cost-risk analysis; cryptanalysis; risk analysis.*

approved circuit

Synonym for *protected wireline distribution system.*

audit

(1) To conduct the independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

(2) The independent review and examination of system activities and records as in (1).

(3) See *external security audit; internal security audit; security audit.*

audit trail

A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

authentication

(1) The act of identifying or verifying the eligibility of a station, originator, or individual to *access* specific categories of information.

(2) A measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator.

authenticator

(1) The means used to identify or verify the eligibility of a station, originator, or individual to *access* specific categories of information.

(2) A symbol, a sequence of symbols, or a series of bits that are arranged in a predetermined manner and are usually inserted at a predetermined point within a message or transmission for the purpose of an *authentication* of the message or transmission.

authorization

The granting to a user, a program, or a process the right of *access.*

automated security monitoring

The use of automated procedures to ensure that the security controls implemented within an ADP system are not circumvented.

backup procedures

The provisions made for the recovery of data files and program libraries, and for restart or replacement of ADP equipment after the occurrence of a system failure or of a disaster.

between-the-lines entry

Access, obtained through the use of *active wiretapping* by an unauthorized user, to a momentarily inactive terminal of a legitimate user assigned to a communications channel.

bounds checking

Testing of computer program results for *access* to storage outside of its authorized limits. Synonymous with memory bounds checking.

bounds register

A hardware register which holds an address specifying a storage boundary.

brevity lists

A *code system* that is used to reduce the length of time required to transmit information by the use of a few characters to represent long, stereotyped sentences.

browsing

Searching through storage to locate or acquire information, without necessarily knowing of the existence or the format of the information being sought.

call back

A procedure established for positively identifying a terminal dialing into a computer system by disconnecting the calling terminal and reestablishing the connection by the computer system's dialing the telephone number of the calling terminal.

certification

The technical evaluation, made as part of and in support of the *accreditation* process, that establishes the extent to which a particular computer system or network design and implementation meet a prespecified set of security requirements.

cipher system

A *cryptographic system* in which *cryptography* is applied to *plain text* elements of equal length.

ciphertext

Unintelligible text or signals produced through the use of *cipher systems*.

code system

(1) Any system of communication in which groups of symbols are used to represent *plain text* elements of varying length.

(2) In the broadest sense, a means of converting information into a form suitable for communications or *encrypion*, for example, coded speech, Morse Code, teletypewriter codes.

(3) A *cryptographic system* in which cryptographic equivalents (usually called code groups) typically consisting of letters, digits, or both in meaningless combinations are substituted for *plain text* elements which may be words, phrases, or sentences.

(4) See also *brevity lists*.

communications security

The protection that insures the authenticity of *telecommunications* and that results from the application of measures taken to deny unauthorized persons information of value which might be derived from the acquisition of telecommunications.

compartmentalization

(1) The isolation of the operating system, user programs, and data files from one another in main storage in order to provide protection against unauthorized or concurrent *access* by other users or programs.

(2) The breaking down of sensitive data into small, isolated blocks for the purpose of reducing risk to the data.

compromise

An unauthorized disclosure or loss of *sensitive information*.

compromising emanations

Electromagnetic emanations that may convey data and that, if intercepted and analyzed, may *compromise sensitive information* being processed by any ADP system.

concealment system

A method of achieving *confidentiality* in which the existence of *sensitive information* is hidden by embedding it in irrelevant data.

confidentiality

A concept that applies to data that must be held in confidence and that describes the status and degree of protection that must be provided for such data about individuals as well as organizations.

control zone

The space, expressed in feet of radius, that surrounds equipment that is used to process *sensitive information* and that is under sufficient physical and technical control to preclude an unauthorized entry or *compromise*. Synonyms with security perimeter.

controlled access

Synonym for *access control*.

controlled accessibility

Synonym for *access control*.

controlled sharing

The condition which exists when *access control* is applied to all users and components of a *resource-sharing* ADP system.

controllable isolation

Controlled sharing in which the scope or domain of *authorization* can be reduced to an arbitrarily small set or sphere of activity.

cost-risk analysis

The assessment of the costs of potential risk of loss or *compromise* of data in an ADP system without data protection versus the cost of providing data protection.

cross-talk

An unwanted transfer of energy from one communications channel to another channel.

cryptanalysis

The steps and operations performed in converting *encrypted* messages into *plain text* without initial knowledge of the *key* employed in the *encryption algorithm*.

cryptographic system

The documents, devices, equipment, and associated techniques that are used as a unit to provide a single means of *encryption* (*enciphering* or *encoding*).

cryptography

The art or science which treats of the principles, means, and methods for rendering *plain text* unintelligible and for converting *encrypted* messsages into intelligible form.

cryptology

The field that encompasses both *cryptography* and *cryptanalysis*.

crypto-operation

See *offline crypto-operation; online crypto-operation*.

data contamination

A deliberate or accidental process or act that results in a change in the integrity of the original data.

200-193 O - 76 - 2

data-dependent protection

Protection of data at a level commensurate with the sensitivity level of the individual data elements, rather than with the sensitivity of the entire file which includes the data elements.

data integrity

The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

data security

The protection of data from accidental or malicious modification, destruction, or disclosure.

data protection engineering

The methodology and tools used for designing and implementing data protection mechanisms.

decipher

To convert, by use of the appropriate *key*, *enciphered* text into its equivalent *plain text*.

decrypt

To convert, by use of the appropriate *key*, *encrypted* (*encoded* or *enciphered*) text into its equivalent *plain text*.

dedicated mode

The operation of an ADP system such that the central computer facility, the connected peripheral devices, the communications facilities, and all remote terminals are used and controlled exclusively by specific users or groups of users for the processing of particular types and categories of information.

degauss

(1) To apply a variable, alternating current (AC) field for the purpose of demagnetizing magnetic recording media, usually tapes. The process involves increasing the AC field gradually from zero to some maximum value and back to zero, which leaves a very low residue of magnetic induction on the media.

(2) Loosely, to erase.

eavesdropping

The unauthorized interception of information-bearing emanations through the use of methods other than wiretapping.

electromagnetic emanations

Signals transmitted as radiation through the air and through conductors.

emanation security

The protection that results from all measures designed to deny unauthorized persons information of value that might be derived from intercept and analysis of *compromising emanations*.

emanations

See *compromising emanations; electromagnetic emanations*.

encipher

To convert *plain text* into unintelligible form by means of a *cipher system*.

encode

To convert *plain text* into unintelligible form by means of a *code system*.

encrypt

To convert *plain text* into unintelligible form by means of a *cryptographic system*.

encryption

See *end-to-end encryption; link encryption*.

encryption algorithm

A set of mathematically expressed rules for rendering information unintelligible by effecting a series of transformations through the use of variable elements controlled by the application of a *key* to the normal representation of the information. Synonymous with privacy transformation.

end-to-end encryption

(1) *Encryption* of information at the origin within a communications network and postponing decryption to the final destination point.

(2) See also *link encryption*.

entrapment

The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit.

entry

See *between-the-lines entry; piggy back entry*.

executive state

One of two generally possible states in which an ADP system may operate, and in which only certain privileged instructions may be executed; such privileged instructions may not be executed when the system is operating in the other, the user state. Synonymous with supervisor state.

external security audit

A *security audit* conducted by an organization independent of the one being *audited*.

failure access

An unauthorized and usually inadvertent *access* to data resulting from a hardware or software failure in the ADP system.

failure control

The methodology used to detect and provide fail-safe or fail-soft recovery from hardware and software failures in an ADP system.

fail safe

The automatic termination and protection of programs or other processing operations when a hardware or software failure is detected in an ADP system.

fail soft

The selective termination of affected non-essential processing when a hardware or software failure is detected in an ADP system.

fault

Synonym for *loophole*.

fetch protection

A system-provided restriction to prevent a program from *accessing* data in another user's segment of storage.

file protection

The aggregate of all processes and procedures established in an ADP system and designed to inhibit unauthorized *access*, *contamination*, or elimination of a file.

flaw

(1) Synonym for *loophole*.

(2) See *pseudo-flaw*.

formulary

A technique for permitting the decision to grant or deny *access* to be determined dynamically at access time, rather than at the time of creation of the *access list*.

handshaking procedures

A dialog between a user and a computer, a computer and another computer, a program and another program for the purpose of identifying a user and authenticating his identity, through a sequence of questions and answers based on information either previously stored in the computer or supplied to the computer by the initiator of dialog. Synonymous with password dialog.

identification

The process that enables, generally by the use of unique machine-readable names, recognition of users or *resources* as identical to those previously described to an ADP system.

impersonation

An attempt to gain *access* to a system by posing as an authorized user. Synonymous with masquerading, mimicking.

incomplete parameter checking

A system fault which exists when all parameters have not been fully checked for correctness and consistency by the operating system, thus making the system vulnerable to penetration.

integrity

See *data integrity; system integrity*.

interactive computing

Use of a computer such that the user is in control and may enter data or make other demands on the system which responds by the immediate processing of user requests and returning appropriate replies to these requests.

interdiction

The act of impeding or denying the use of system *resources* to a user.

internal security audit

A *security audit* conducted by personnel responsible to the management of the organization being *audited*.

isolation

The containment of users and resources in an ADP system in such a way that users and processes are separate from one another as well as from the protection controls of the operating system.

key

In *cryptography*, a sequence of symbols that controls the operations of *encryption* and *decryption*.

key generation

The origination of a *key* or of a set of distinct keys.

keyword

Synonym for *password*.

linkage

The purposeful combination of data or information from one information system with that from another system in the hope of deriving additional information; in particular, the combination of computer files from two or more sources.

link encryption

(1) The application of *online crypto-operations* to a link of a communications system so that all information passing over the link is *encrypted* in its entirety.

(2) *End-to-end encryption* within each link in a communications network.

lock-and-key protection system

A protection system that involves matching a *key* or *password* with a specified *access* requirement.

logical completeness measure

A means for assessing the effectiveness and degree to which a set of security and *access control mechanisms* meets the requirements of a set of security specifications.

loophole

An error of omission or oversight in software or hardware which permits circumventing the *access control* process. Synonymous with fault, flaw.

masquerading

Synonym for *impersonation*.

memory bounds

The limits in the range of storage addresses for a protected region in memory.

memory bounds checking

Synonym for *bounds checking*.

mimicking

Synonym for *impersonation*.

monitoring

See *automated security monitoring; threat monitoring*.

multiple access rights terminal

A terminal that may be used by more than one class of users; for example, users with different *access* rights to data.

mutually suspicious

Pertaining to the state that exists between interactive processes (subsystems or programs) each of which contains sensitive data and is assumed to be designed so as to extract data from the other and to protect its own data.

nak attack

A *penetration* technique which capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly and, thus, leaves the system in an unprotected state during such interrupts.

offline crypto-operation

Encryption or *decryption* performed as a self-contained operation distinct from the transmission of the encrypted text, as by hand or by machines not electrically connected to a signal line.

online crypto-operation

The use of crypto-equipment that is directly connected to a signal line, making single continuous processes of *encryption* and transmission or reception and *decryption*.

overwriting

The obliteration of recorded data by recording different data on the same surface.

passive wiretapping

The monitoring and/or recording of data while the data is being transmitted over a communications link.

password

A protected word or a string of characters that identifies or *authenticates* a user, a specific *resource*, or an *access type*. Synonymous with keyword.

password dialog

Synonym for *handshaking procedure*.

penetration

A successful unauthorized *access* to an ADP system.

penetration profile

A delineation of the activities required to effect a *penetration*.

penetration signature

(1) The description of a situation or set of conditions in which a *penetration* could occur.

(2) The description of usual and unusual system events which in conjunction can indicate the occurrence of a *penetration* in progress.

penetration testing

The use of special programmer/analyst teams to attempt to *penetrate* a system for the purpose of identifying any security weaknesses.

personnel security

The procedures established to insure that all personnel who have *access* to any *sensitive information* have the required authorities as well as all appropriate clearances.

physical security

(1) The use of locks, guards, badges, and similar administrative measures to control *access* to the computer and related equipment.

(2) The measures required for the protection of the structures housing the computer, related equipment and their contents from damage by accident, fire, and environmental hazards.

piggy back entry

Unauthorized *access* that is gained to an ADP system via another user's legitimate connection.

plain text

Intelligible text or signals that have meaning and that can be read or acted upon without the application of any *decryption*.

principle of least privilege

The granting of the minimum *access authorization* necessary for the performance of required tasks.

print suppress

To eliminate the printing of characters in order to preserve their secrecy; for example, the characters of a *password* as it is keyed by a user at an input terminal.

privacy

(1) The right of an individual to self-determination as to the degree to which the individual is willing to share with others information about himself that may be *compromised* by unauthorized exchange of such information among other individuals or organizations.

(2) The right of individuals and organizations to control the collection, storage, and dissemination of their information or information about themselves.

privacy protection

The establishment of appropriate administrative, technical, and physical safeguards to ensure the *security* and *confidentiality* of *data* records and to protect both security and confidentiality against any anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom such information is maintained.

privacy transformation

Synonym for *encryption algorithm*.

privileged instructions

(1) A set of instructions generally executable only when the ADP system is operating in the *executive state*; for example, the handling of interrupts.

(2) Special computer instructions designed to control the protection features of an ADP system; for example, the storage protection features.

procedural security

Synonym for *administrative security*.

procedures

See *backup procedures; handshaking procedures; recovery procedures; system integrity procedures*.

protected wireline distribution system

A *telecommunications* system which has been approved by a legally designated authority and to which electromagnetic and physical safeguards have been applied to permit safe electrical transmission of unencrypted *sensitive information*. Synonymous with approved circuit.

protection

See *data-dependent protection; fetch protection; file protection; lock-and-key protection system; privacy protection*.

protection ring

One of a hierarchy of privileged modes of an ADP system that gives certain *access* rights to the users, programs, and processes authorized to operate in a given mode.

pseudo-flaw

An apparent *loophole* deliberately implanted in an operating system program as a trap for intruders.

purging

(1) The orderly review of storage and removal of inactive or obsolete data files.

(2) The removal of obsolete data by erasure, by *overwriting* of storage, or by resetting registers.

real-time reaction

A response to a *penetration* attempt which is detected and diagnosed in time to prevent the actual penetration.

recovery procedures

The actions necessary to restore a system's computational capability and data files after a system failure or *penetration*.

remanence

The residual magnetism that remains on magnetic storage media after *degaussing*.

residue

Data left in storage after processing operations, and before *degaussing* or rewriting has taken place.

resource

In an ADP system, any function, device, or data collection that may be allocated to users or programs.

resource sharing

In an ADP system, the concurrent use of a *resource* by more than one user, job or program.

risk analysis

An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events.

sanitizing

The *degaussing* or *overwriting* of *sensitive information* in magnetic or other storage media. Synonymous with scrubbing.

scavenging

Searching through *residue* for the purpose of unauthorized data acquisition.

scrubbing

Synonym for *sanitizing.*

secure configuration management

The use of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of insuring that such changes will not lead to a decreased *data security.*

secure operating system

An operating system that effectively controls hardware and software functions in order to provide the level of protection appropriate to the value of the data and *resources* managed by the operating system.

security

See *add-on security; administrative security; communications security; data security; emanation security; personnel security; physical security;* procedural security; teleprocessing security; *traffic flow security.*

security audit

An examination of *data security* procedures and measures for the purpose of evaluating their adequacy and compliance with established policy.

security filter

A set of sofeware routines and techniques employed in ADP systems to prevent automatic forwarding of specified data over unprotected links or to unauthorized persons.

security kernel

The central part of a computer system (software and hardware) that implements the fundamental security procedures for *controlling access* to system *resources.*

security perimeter

Synonym for *control zone.*

seepage

The accidental flow, to unauthorized individuals, of data or information *access* to which is presumed to be controlled by computer security safeguards.

sensitive information

Any information which requires a degree of protection and which should not be made generally available.

spoofing

The deliberate inducement of a user or a *resource* to take an incorrect action.

supervisor state

Synonym for *executive state.*

system

See *cipher system; code system; concealment system; cryptographic system; lock-and-key protection system; protected wireline distribution system; secure operating system.*

system integrity

The state that exists when there is complete assurance that under all conditions an ADP system is based on the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that implement the protection mechanisms, and *data integrity.*

system integrity procedures

The procedure established for assurring that the hardware, software, and data in an ADP system maintain their state of original integrity and are not tampered with by program changes.

technological attack

An attack which can be perpetrated by circumventing or nullifying hardware and software *access control mechanisms,* rather than by subverting system personnel or other users.

telecommunications

Any transmission, emission, or reception of signs, signals, writing, images, sounds or other information by wire, radio, visual, or any electromagnetic systems.

teleprocessing

Pertaining to an information transmission system that combines *telecommunications,* ADP systems, and man-machine interface equipment for the purpose of interacting and functioning as an integrated whole.

teleprocessing security

The protection that results from all measures designed to prevent deliberate, inadvertent, or unauthorized disclosure, acquisition, manipulation, or modification of information in a *teleprocessing* system.

terminal identification

The means used to establish the unique identification of a terminal by an ADP system.

threat monitoring

The analysis, assessment, and review of *audit trails* and other data collected for the purpose of searching out system events which may constitute violations or precipitate incidents involving data *privacy* matters.

time-dependent password

A *password* which is valid only at a certain time of the day or during a specified interval of time.

traffic flow security

The protection that results from those features in some crypto-equipment that conceal the presence of valid messages on a communications circuit, usually by causing the circuit to appear busy at all times, or by *encrypting* the source and destination addresses of valid messages.

trap door

A breach created intentionally in an ADP system for the purpose of collecting, altering or destroying data.

trojan horse

A computer program that is apparently or actually useful and that contains a *trap door*.

validation

The performance of tests and evaluations in order to determine compliance with security specifications and requirements.

wiretapping

See *active wiretapping, passive wiretapping.*

work factor

An estimate of the effort or time that can be expected to be expended to overcome a protective measure by a would-be penetrator with specified expertise and *resources.*

APPENDIX A. Other Relevant Computer Security and Privacy Publications

Controlled Accessibility Bibliography (NBS Technical Note 780; June, 1973)	A bibliography of works dealing with the hardware and software technological measures available in a computer system for the protection of data.	Superintendent of Documents U.S. Government Printing Office Washington, D.C. 20402	C13.46:780	$ .55
Controlled Accessibility Workshop Report (NBS Technical Note 827; May, 1974)	A report of the NBS/ACM Workshop on Controlled Accessibility, December 1972, Rancho Santa Fe, California. The workshop was divided into five separate working groups: access controls, audit, EDP management controls, identification, and measurements. The report contains the introductory remarks outlining the purpose and goals of the workshop, summaries of the discussions that took place in the working groups and the conclusions that were reached.	Superintendent of Documents U.S. Government Printing Office Washington, D.C. 20402	C13.46:827	$1.25
Executive Guide to Computer Security (NBS Special Publication; May, 1974)	This booklet was prepared for non-ADP executives and managers. It is intended to introduce management to the necessity for computer security and the problems encountered in providing for it.	Systems and Software Division Room A247, Technology Bldg. National Bureau of Standards Washington, D.C. 20234	None	No Charge
Guidelines for Physical Security and Risk Management (Federal Information Processing Standards Publication 31; June, 1974)	This publication provides guidelines to be used by Federal organizations in structuring physical security programs for their ADP facilities. It treats risk analysis, natural disasters, supporting utilities, systems reliability, procedural measures and controls, off-site facilities, contingency plans, security awareness and security audit. Statistics and information relevant to physical security of computer data and facilities are presented. There are also many references to other, applicable publications containing more exhaustive treatments of specific subjects.	Superintendent of Documents U.S. Government Printing Office Washington, D.C. 20402	C13.52:31	$1.35
Computer Security Guidelines for Implementing the Privacy Act of 1974 (Federal Information Processing Standards Publication 41; 1975 May 30)	This publication provides guidelines for use by Federal ADP organizations in implementing the computer security safeguards necessary for compliance with Public Law 93-579, the Privacy Act of 1974. A wide variety of technical and related procedural safeguards are described. These fall into three broad categories: Physical security, information management practices, and computer system/network security controls. As each organization processing personal data has unique characteristics, specific organizations should draw upon the material provided in order to select a well-balanced combination of safeguards which meets their particular requirements.	Superintendent of Documents U.S. Government Printing Office Washington, D.C. 20402	C13.52:41	$ .70

U.S. GOVERNMENT PRINTING OFFICE 1976 O - 200-198

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH reports National Bureau of Standards research and development in physics, mathematics, and chemistry. It is published in two sections, available separately:

o Physics and Chemistry (Section A)

Papers of interest primarily to scientists working in these fields. This section covers a broad range of physical and chemical research, with major emphasis on standards of physical measurement, fundamental constants, and properties of matter. Issued six times a year. Annual subscription: Domestic, $17.00; Foreign, $21.25.

o Mathematical Sciences (Section B)

Studies and compilations designed mainly for the mathematician and theoretical physicist. Topics in mathematical statistics, theory of experiment design, numerical analysis, theoretical physics and chemistry, logical design and programming of computers and computer systems. Short numerical tables. Issued quarterly. Annual subscription: Domestic, $9.00; Foreign, $11.25.

DIMENSIONS/NBS (formerly Technical News Bulletin)—This monthly magazine is published to inform scientists, engineers, businessmen, industry, teachers, students, and consumers of the latest advances in science and technology, with primary emphasis on the work at NBS. The magazine highlights and reviews such issues as energy research, fire protection, building technology, metric conversion, pollution abatement, health and safety, and consumer product performance. In addition, it reports the results of Bureau programs in measurement standards and techniques, properties of matter and materials, engineering standards and services, instrumentation, and automatic data processing.

Annual subscription: Domestic, $9.45; Foreign, $11.85.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a world-wide program coordinated by NBS. Program under authority of National Standard Data Act (Public Law 90-396).

NOTE: At present the principal publication outlet for these data is the Journal of Physical and Chemical Reference Data (JPCRD) published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements available from ACS, 1155 Sixteenth St. N. W., Wash. D. C. 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The purpose of the standards is to establish nationally recognized requirements for products, and to provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Federal Information Processing Standards Publications (FIPS PUBS)—Publications in this series collectively constitute the Federal Information Processing Standards Register. Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service (Springfield, Va. 22161) in paper copy or microfiche form.

Order NBS publications (except NBSIR's and Bibliographic Subscription Services) from: Superintendent of Documents, Government Printing Office, Washington, D.C. 20402.

BIBLIOGRAPHIC SUBSCRIPTION SERVICES

The following current-awareness and literature-survey bibliographies are issued periodically by the Bureau:

Cryogenic Data Center Current Awareness Service

A literature survey issued biweekly. Annual subscription: Domestic, $20.00; foreign, $25.00.

Liquefied Natural Gas. A literature survey issued quarterly. Annual subscription: $20.00.

Superconducting Devices and Materials. A literature survey issued quarterly. Annual subscription: $20.00. Send subscription orders and remittances for the preceding bibliographic services to National Bureau of Standards, Cryogenic Data Center (275.02) Boulder, Colorado 80302.

Electromagnetic Metrology Current Awareness Service

Issued monthly. Annual subscription: $24.00. Send subscription order and remittance to Electromagnetics Division, National Bureau of Standards, Boulder, Colo. 80302.