NCSC-TG-004-88
Library No. S-231,238

FOREWORD

This publication, "Glossary of Computer Security Terms," is issued by the National Computer Security Center (NCSC) under the authority of and in accordance with Department of Defense (DoD) Directive 5215.1, "Computer Security Evaluation Center." The definitions in this glossary are intended for use by U.S. Government agencies or contractors that apply the criteria of DoD Directive 5200.28-STD, "DoD Trusted Computer System Evaluation Criteria," in the use of their computer systems.

Recommendations for revision to this publication are encouraged and will be reviewed periodically by the NCSC. Address all proposals for revision through appropriate channels to:

National Computer Security Center
9800 Savage Road
Fort George G. Meade, MD 20755-6000
Attention: Chief, Criteria and Technical Guidelines Division

21 October 1988

Patrick R. Gallagher, Jr.
Director
National Computer Security Center

For sale by the Superintendent of Documents, Congressional Sales Office, U.S. Government Printing Office, Washington, DC 20402

ACKNOWLEDGMENTS

Recognition is extended to Sue Berg as primary researcher for this glossary, Carol Lane as the initial editor, and to Mary Whittaker as final researcher and editor. Appreciation is extended to all who contributed and refined the definitions, particularly Devolyn Duggar and Maj. Douglas Hardie, USAF.

PREFACE

This glossary contains material drawn primarily from official documents of the United States Government departments and agencies. Other terms are from private organizations and individuals, as indicated in the Reference section at the end of this document.

The intent of the National Computer Security Center is for this document to focus on terms in the field of computer security. However, because of the overlap of computer security and other security disciplines, some terms such as *TEMPEST* are included.

TABLE OF CONTENTS

GLOSSARY OF COMPUTER SECURITY ACRONYMS

AIS	Automated Information System
COMPUSEC	Computer Security
COMSEC	Communications Security
CSTVRP	Computer Security Technical Vulnerability Reporting Program
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DES	Data Encryption Standard
DPL	Degausser Products List
DTLS	Descriptive Top-Level Specification
EPL	Evaluated Products List
ETL	Endorsed Tools List
FTLS	Formal Top-Level Specification
ISSO	Information System Security Officer
MAC	Mandatory Access Control
NCSC	National Computer Security Center
NTISSC	National Telecommunications and Information Systems Security Committee
OPSEC	Operations Security
PPL	Preferred Products List
SAISS	Subcommittee on Automated Information Systems Security of NTISSC
SSO	System Security Officer
STS	Subcommittee on Telecommunications Security of NTISSC
TCB	Trusted Computing Base
TCSEC	*DoD Trusted Computer System Evaluation Criteria*

GLOSSARY OF COMPUTER SECURITY TERMS

-*-

***-property (or star property)**

A Bell-La Padula security model rule allowing a subject write access to an object only if the security level of the object dominates the security level of the subject. Also called confinement property.

-A-

acceptance inspection

The final inspection to determine whether or not a facility or system meets the specified technical and performance standards. Note: This inspection is held immediately after facility and software testing and is the basis for commissioning or accepting the information system.

access

A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

access control

The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network. Synonymous with *controlled access* and *limited access.*

access control mechanism

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 in an automated system.

access level

The hierarchical portion of the security level used to identify the sensitivity of data and the clearance or authorization of users. Note: The access level, in conjunction with the nonhierarchical categories, forms the sensitivity label of an object. See *category, security level*, and *sensitivity label*.

access list

A list of users, programs, and/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 port

A logical or physical identifier that a computer uses to distinguish different terminal input/output data streams.

access type

The nature of an access right to a particular device, program, or file (e.g., read, write, execute, append, modify, delete, or create).

accountability

The property that enables activities on a system to be traced to individuals who may then be held responsible for their actions.

accreditation

A formal declaration by the DAA that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

accreditation authority

Synonymous with *Designated Approving Authority*.

add-on security

The retrofitting of protection mechanisms, implemented by hardware or software.

administrative security

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

assurance

A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy.

attack

The act of trying to bypass security controls on a system. An attack may be active, resulting in the alteration of data; or passive, resulting in the release of data. Note: The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures.

audit trail

A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.

authenticate

(1) To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

(2) To verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.

authenticator

The means used to confirm the identity or to verify the eligibility of a station, originator, or individual.

authorization

The granting of access rights to a user, program, or process.

automated data processing security

Synonymous with *automated information systems security.*

automated information system (AIS)

An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

automated information system security

Measures and controls that protect an AIS against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data. AIS security includes consideration of all hardware and/or software functions, characteristics and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable protection level for an AIS and for data handled by an AIS.

automated security monitoring

The use of automated procedures to ensure that security controls are not circumvented.

availability of data

The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.

-B-

back door

Synonymous with *trap door.*

backup plan

Synonymous with *contingency* pIan.

Bell-La Padula model

A formal state transition model of computer security policy that describes a set of access control rules. In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of a secure state is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby inductively proving that the system is secure. A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a specific security policy. In order to determine whether or not a specific access mode is allowed, the clearance of a subject is compared to the classification of the object, and a determination is made as to whether the subject is authorized for the specific access mode. See *star property (*-property)* and *simple security property.*

benign environment

A nonhostile environment that may be protected from external hostile elements by physical, personnel, and procedural security countermeasures.

between-the-lines entry

Unauthorized access obtained by tapping the temporarily inactive terminal of a legitimate user. See *piggy back.*

beyond A1

A level of trust defined by the *DoD Trusted Computer System Evaluation Criteria (TCSEC)* that is beyond the state-of-the-art technology available at the time the criteria were developed. It includes all the A1-level features plus additional ones not required at the A1 level.

browsing

The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought.

-C-

call back

A procedure for identifying a remote terminal. In a call back, the host system disconnects the caller and then dials the authorized telephone number of the remote terminal to reestablish the connection. Synonymous with *dial back.*

capability

A protected identifier that both identifies the object and specifies the access rights to be allowed to the accessor who possesses the capability. In a capability-based system, access to protected objects such as files is granted if the would-be accessor possesses a capability for the object.

category

A restrictive label that has been applied to classified or unclassified data as a means of increasing the protection of the data and further restricting access to the data.

certification

The comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

closed security environment

An environment in which both of the following conditions hold true:

(1) Application developers (including maintainers) have sufficient clearances and authorizations to provide an acceptable presumption that they have not introduced malicious logic. (2) Configuration control provides sufficient assurance that applications and the equipment are protected against the introduction of malicious logic prior to and during the operation of system applications.

communications security (COMSEC)

Measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government concerning national security, and to ensure the authenticity of such telecommunicatons. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security material and information.

compartment

A class of information that has need-to-know access controls beyond those normally provided for access to Confidential, Secret or Top Secret information.

compartmented security mode

See *modes of operation.*

compromise

A violation of the security policy of a system such that unauthorized disclosure of sensitive information may have occurred.

compromising emanations

Unintentional data-related or intelligence-bearing signals that, if intercepted and analyzed, disclose the information transmission received, handled, or otherwise processed by any information processing equipment. See *TEMPEST*.

computer abuse

The misuse, alteration, disruption or destruction of data processing resources. The key aspect is that it is intentional and improper.

computer cryptography

The use of a crypto-algorithm in a computer, microprocessor, or microcomputer to perform encryption or decryption in order to protect information or to authenticate users, sources, or information.

computer fraud

Computer-related crimes involving deliberate misrepresentation, alteration or disclosure of data in order to obtain something of value (usually for monetary gain). A computer system must have been involved in the perpetration or coverup of the act or series of acts. A computer system might have been involved through improper manipulation of input data; output or results; applications programs; data files; computer operations; communications; or computer hardware, systems software, or firmware.

computer security (COMPUSEC)

Synonymous with *automated information systems security*.

computer security subsystem

A device designed to provide limited computer security features in a larger system environment.

Computer Security Technical Vulnerability Reporting Program (CSTVRP)

A program that focuses on technical vulnerabilities in commercially available hardware, firmware and software products acquired by DoD. CSTVRP provides for the reporting, cataloging, and discreet dissemination of technical vulnerability and corrective measure information to DoD components on a need-to-know basis.

concealment system

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

confidentiality

The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.

configuration control

The process of controlling modifications to the system's hardware, firmware, software, and documentation that provides sufficient assurance that the system is protected against the introduction of improper modifications prior to, during, and after system implementation. Compare *configuration management.*

configuration management

The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures and test documentation throughout the development and operational life of the system. Compare *configuration control*.

confinement

The prevention of the leaking of sensitive data from a program.

confinement channel

Synonymous with *covert channel*.

confinement property

Synonymous with *star property (*-property).*

contamination

The intermixing of data at different sensitivity and need-to-know levels. The lower level data is said to be contaminated by the higher level data; thus, the contaminating (higher level) data may not receive the required level of protection.

contingency plan

A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Synonymous with *disaster plan and emergency plan*.

control zone

The space, expressed in feet of radius, surrounding equipment processing sensitive information, that is under sufficient physical and technical control to preclude an unauthorized entry or compromise.

controlled access

See *access control.*

controlled sharing

The condition that exists when access control is applied to all users and components of a system.

cost-risk analysis

The assessment of the costs of providing data protection for a system versus the cost of losing or compromising the data.

countermeasure

Any action, device, procedure, technique, or other measure that reduces the vulnerability of or threat to a system.

covert channel

A communications channel that allows two cooperating processes to transfer information in a manner that violates the system's security policy. Synonymous with *confinement channel*.

covert storage channel

A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

covert timing channel

A covert channel in which one process signals information to another by modulating its own use of system resources (e.g., CPU time) in such a way that this manipulation affects the real response time observed by the second process.

Criteria

See *DoD Trusted Computer System Evaluation Criteria*.

crypto-algorithm

A well-defined procedure or sequence of rules or steps used to produce a key stream or cipher text from plain text and vice versa.

cryptography

The principles, means and methods for rendering information unintelligible, and for restoring encrypted information to intelligible form.

cryptosecurity

The security or protection resulting from the proper use of technically sound cryptosystems.

-D-

Data Encryption Standard (DES)

A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology, is intended for public and government use.

data flow control

Synonymous with *information flow control*.

data integrity

The property that data meet an a priori expectation of quality.

data security

The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

declassification of AIS storage media

An administrative decision or procedure to remove or reduce the security classification of the subject media.

dedicated security mode

See *modes of operation*.

default classification

A temporary classification reflecting the highest classification being processed in a system. The default classification is included in the caution statement affixed to the object.

degauss

To reduce magnetic flux density to zero by applying a reverse magnetizing field.

degausser

An electrical device that can generate a magnetic field for the purpose of degaussing magnetic storage media.

Degausser Products List (DPL)

A list of commercially produced degaussers that meet National Security Agency specifications. This list is included in the *NSA Information Systems Security Products and Services Catalogue*, and is available through the Government Printing Office.

denial of service

Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service. Synonymous with *interdiction*.

Descriptive Top-Level Specification (DTLS)

A top-level specification that is written in a natural language (e.g., English), an informal design notation, or a combination of the two.

Designated Approving Authority (DAA)

The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

dial back

Synonymous with *call back*.

dial-up

The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer.

disaster plan

Synonymous with *contingency plan*.

discretionary access control (DAC)

A means of restricting access to objects based on the identity and need-to-know of the user, process and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject. Compare *mandatory access control*.

DoD Trusted Computer System Evaluation Criteria (TCSEC)

A document published by the National Computer Security Center containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built into systems. These criteria are intended for use in the design and evaluation of systems that will process and/or store sensitive or classified data. This document is Government Standard DoD 5200.28-STD and is frequently referred to as "*The Criteria*" or "*The Orange Book*."

domain

The unique context (e.g., access control parameters) in which a program is operating; in effect, the set of objects that a subject has the ability to access. See process and subject.

dominate

Security level S_1 is said to dominate security level S_2 if the hierarchical classification of S_1 is greater than or equal to that of S_2 and the nonhierarchical categories of S_1 include all those of S_2 as a subset.

-E-

emanations

See *compromising emanations.*

embedded system

A system that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem.

emergency plan

Synonymous with *contingency pIan*.

emission security

The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and from an analysis of compromising emanations from systems.

end-to-end encryption

The protection of information passed in a telecommunications system by cryptographic means, from point of origin to point of destination.

Endorsed Tools List (ETL)

The list of formal verification tools endorsed by the NCSC for the development of systems with high levels of trust.

Enhanced Hierarchical Development Methodology

An integrated set of tools designed to aid in creating, analyzing, modifying, managing, and documenting program specifications and proofs. This methology includes a specification parser and type checker, a theorem prover, and a multi-level security checker. Note: This methodology is <u>not</u> based upon the Hierarchical Development Methodology.

entrapment

The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations.

environment

The aggregate of external procedures, conditions, and objects that affect the development, operation, and maintenance of a system.

erasure

A process by which a signal recorded on magnetic media is removed. Erasure is accomplished in two ways: (1) by alternating current erasure, by which the information is destroyed by applying an alternating high and low magnetic field to the media; or (2) by direct current erasure, by which the media are saturated by applying a unidirectional magnetic field.

Evaluated Products List (EPL)

A list of equipments, hardware, software, and/or firmware that have been evaluated against, and found to be technically compliant, at a particular level of trust, with the DoD TCSEC by the NCSC. The EPL is included in the *National Security Agency Information Systems Security Products* and *Services Catalogue*, which is available through the Government Printing Office.

executive state

One of several states in which a system may operate and the only one in which certain privileged instructions may be executed. Such instructions cannot be executed when the system is operating in other (e.g., user) states. Synonymous with *supervisor state*.

exploitable channel

Any information channel that is usable or detectable by subjects external to the trusted computing base whose purpose is to violate the security policy of the system. See *covert channel.*

-F-

failsafe

Pertaining to the automatic protection of programs and/or processing systems to maintain safety when a hardware or software failure is detected in a system.

failsoft

Pertaining to the selective termination of affected nonessential processing when a hardware or software failure is detected in a system.

failure access

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

failure control

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

fault

A condition that causes a device or system component to fail to perform in a required manner.

fetch protection

A system-provided restriction to prevent a program from accessing data in another users segment of storage.

file protection

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

file security

The means by which access to computer files is limited to authorized users only.

flaw hypothesis methodology

A systems analysis and penetration technique in which specifications and documentation for the system are analyzed and then flaws in the system are hypothesized. The list of hypothesized flaws is then prioritized on the basis of the estimated probability that a flaw exists and, assuming a flaw does exist, on the ease of exploiting it, and on the extent of control or compromise it would provide. The prioritized list is used to direct a penetration attack against the system.

flow control

See *information flow control*.

formal access approval

Documented approval by a data owner to allow access to a particular category of information.

Formal Development Methodology

A collection of languages and tools that enforces a rigorous method of verification. This methodology uses the Ina Jo specification language for successive stages of system development, including identification and modeling of requirements, high-level design, and program design.

formal proof

A complete and convincing mathematical argument, presenting the full logical justification for each proof step, for the truth of a theorem or set of theorems.

formal security policy model

A mathematically precise statement of a security policy. To be adequately precise, such a model must represent the initial state of a system, the way in which the system progresses from one state to another, and a definition of a “secure” state of the system. To be acceptable as a basis for a TCB, the model must be supported by, a formal proof that if the initial state of the system satisfies the definition of a “secure" state and if all assumptions required by the model hold, then all future states of the system will be secure. Some formal modeling techniques include: state transition models, denotational semantics models, and algebraic specification models. See *Bell-La Padula model* and *security policy model.*

Formal Top-Level Specification (FTLS)

A top-level specification that is written in a formal mathematical language to allow theorems showing the correspondence of the system specification to its formal requirements to be hypothesized and formally proven.

formal verification

The process of using formal proofs to demonstrate the consistency between a formal specification of a system and a formal security policy model (design verification) or between the formal specification and its high level program implementation (implementation verification).

front-end security filter

A security filter, which could be implemented in hardware or software, that is logically separated from the remainder of the system to protect the system's integrity.

functional testing

The segment of security testing in which the advertised security mechanisms of the system are tested, under operational conditions, for correct operation.

-G-

granularity

An expression of the relative size of a data object; e.g., protection at the file level is considered coarse granularity, whereas protection at field level is considered to be of a finer granularity.

guard

A processor that provides a filter between two disparate systems operating at different security levels or between a user terminal and a data base to filter out data that the user is not authorized to access.

Gypsy Verification Environment

An integrated set of tools for specifying, coding, and verifying programs written in the Gypsy language, a language similar to Pascal which has both specification and programming features. This methology includes an editor, a specification processor, a verification condition generator, a user-directed theorem prover, and an information flow tool.

-H-

handshaking procedure

A dialogue between two entities (e.g., a user and a computer, a computer and another computer, or a program and another program) for the purpose of identifying and authenticating the entities to one another.

Hierarchical Development Methodology

A methodology for specifying and verifying the design programs written in the Special specification language. The tools for this methodology include the Special specification processor, the Boyer-Moore theorem prover, and the Feiertag information flow tool.

host to front-end protocol

A set of conventions governing the format and control of data that are passed from a host to a front-end machine.

-I-

identification

The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

impersonating

Synonymous with *spoofing*.

incomplete parameter checking

A system design flaw that results when all parameters have not been fully anticipated for accuracy and consistency, thus making the system vulnerable to penetration.

individual accountability

The ability to associate positively the identity of a user with the time, method, and degree of access to a system.

information flow control

A procedure to ensure that information transfers within a system are not made from a higher security level object to an object of a lower security level. See *covert channel, simple security property, star property (*-property).* Synonymous with *data flow control* and *flow control.*

Information System Security Officer (ISSO)

The person responsible to the DAA for ensuring that security is provided for and implemented throughout the life cycle of an AIS from the beginning of the concept development plan through its design, development, operation, maintenance, and secure disposal.

Information Systems Security Products and Services Catalogue

A catalogue issued quarterly by the National Security Agency that incorporates the DPL, EPL, ETL, PPL and other security product and service lists. This catalogue is available through the U.S. Government Printing Office, Washington, DC 20402, (202)783-3238.

integrity

Sound, unimpaired or perfect condition.

interdiction

See *denial of service*.

internal security controls

Hardware, firmware, and software features within a system that restrict access to resources (hardware, software, and data) to authorized subjects only (persons, programs, or devices).

isolation

The containment of subjects and objects in a system in such a way that they are separated from one another, as well as from the protection controls of the operating system.

-J-

This document contains no entries beginning with the letter "J".

-K-

This document contains no entries beginning with the letter “K”.

-L-

least privilege

The principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

limited access

Synonymous with *access control.*

list-oriented

A computer protection system in which each protected object has a list of all subjects authorized to access it. Compare *ticket-oriented.*

lock-and-key protection system

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

logic bomb

A resident computer program that triggers the perpetration of an unauthorized act when particular states of the system are realized.

loophole

An error of omission or oversight in software or hardware that permits circumventing the system security policy.

-M-

magnetic remanence

A measure of the magnetic flux density remaining after removal of the applied magnetic force. Refers to any data remaining on magnetic storage media after removal of the power.

maintenance hook

Special instructions in software to allow easy maintenance and additional feature development. These are not clearly defined during access for design specification. Hooks frequently allow entry into the code at unusual points or without the usual checks, so they are a serious security risk if they are not removed prior to live implementation. Maintenance hooks are special types of trap doors.

malicious logic

Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose; e.g., a Trojan horse.

mandatory access control (MAC)

A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i. e., clearance) of subjects to access information of such sensitivity. Compare *discretionary access control.*

masquerading

Synonymous with *spoofing*.

mimicking

Synonymous with *spoofing*.

modes of operation

A description of the conditions under which an AIS functions, based on the sensitivity of data processed and the clearance levels and authorizations of the users. Four modes of operation are authorized:

(1) Dedicated Mode
An AIS is operating in the dedicated mode when each user with direct or indirect individual access to the AIS, its peripherals, remote terminals, or remote hosts, has all of the following:

a. A valid personnel clearance for all information on the system.
b. Formal access approval for, and has signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs).
c. A valid need-to-know for all information contained within the system.

(2) System-High Mode
An AS is operating in the system-high mode when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following:

a. A valid personnel clearance for all information on the AIS.
b. Formal access approval for, and has signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs).
c. A valid need-to-know for some of the information contained within the AIS.

(3) Compartmented Mode
An AIS is operating in the compartmented mode when each user with direct or indirect access to AIS, its peripherals, remote terminals, or remote hosts, has all of the following.
a. A valid personnel clearance for the most restricted information processed in the AIS.
b. Formal access approval for, and has signed nondisclosure agreements for that information to which he/she is to have access.
c. A valid need-to-know for that information to which he/she is to have access.

(4) Multilevel Mode
An AIS is operating in the multilevel mode when all the following statements are satisfied concerning the users with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts:
a. Some do not have a valid personnel clearance for all the information processed in the AIS.
b. All have the proper clearance and have the appropriate formal access approval for that information to which he/she is to have access.
c. All have a valid need-to-know for that information to which they are to have access.

multilevel device

A device that is used in a manner that permits it to simultaneously process data of two or more security levels without risk of compromise. To accomplish this, sensitivity labels are normally stored on the same physical medium and in the same form (i.e., machine-readable or human-readable) as the data being processed.

multilevel secure

A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization.

multilevel security mode

See *modes of operation*.

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.

multiuser mode of operation

A mode of operation designed for systems that process sensitive unclassified information in which users may not have a need-to-know for all information processed in the system. This mode is also for microcomputers processing sensitive unclassified information that cannot meet the requirements of the stand-alone mode of operation.

mutually suspicious

The state that exists between interacting processes (subsystems or programs) in which neither process can expect the other process to function securely with respect to some property.

-N-

National Computer Security Assessment Program

A program designed to evaluate the interrelationship of empirical data of computer security infractions and critical systems profiles, while comprehensively incorporating information from the CSTVRP. The assessment will build threat and vulnerability scenarios that are based on a collection of facts from relevant reported cases. Such scenarios are a powerful, dramatic, and concise form of representing the value of loss experience analysis.

National Computer Security Center (NCSC)

Originally named the DoD Computer Security Center, the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the Federal Government.

National Security Decision Directive 145 (NSDD 145)

Signed by President Reagan on 17 September 1984, this directive is entitled "National Policy on Telecommunications and Automated Information Systems Security." It provides initial objectives, policies, and an organizational structure to guide the conduct of national activities toward safeguarding systems that process, store, or communicate sensitive information; establishes a mechanism for policy development; and assigns implementation responsibilities.

National Telecommunications and Information Systems Security Advisory Memoranda/Instructions (NTISSAM, NTISSI)

NTISS Advisory Memoranda and Instructions provide advice, assistance, or information of general interest on telecommunications and systems security to all applicable federal departments and agencies. NTISSAMs/NTISSIs are promulgated by the National Manager for Telecommunications and Automated Information Systems Security and are recommendatory.

National Telecommunications and Information System Security Directives (NTISSD)

NTISS Directives establish national-level decisions relating to NTISS policies, plans, programs, systems, or organizational delegations of authority. NTISSDs are promulgated by the Executive Agent of the Government for Telecommunications and Information Systems Security, or by the Chairman of the NTISSC when so delegated by the Executive Agent. NTISSDs are binding upon all federal departments and agencies.

need-to-know

The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

network front end

A device that implements the necessary network protocols, including security-related protocols, to allow a computer system to be attached to a network.

NSDD 145

See *National Security Decision Directive 145*.

-O-

object

A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes.

object reuse

The reassignment and reuse of a storage medium (e.g., page frame, disk sector, magnetic tape) that once contained one or more objects. To be securely reused and assigned to a new subject, storage media must contain no residual data (magnetic remanence) from the object(s) previously contained in the media.

open security environment

An environment that includes those systems in which at least one of the folIowing conditions holds true: (l) Application developers (including maintainers) do not have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic. (2) Configuration control does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications.

Operations Security (OPSEC)

An analytical process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations.

Orange Book

Alternate name for *DoD Trusted Computer Security Evaluation Criteria*.

overt channel

A path within a computer system or network that is designed for the authorized transfer of data. Compare *covert channel*.

overwrite procedure

A stimulation to change the state of a bit followed by a known pattern. See *magnetic remanence*.

-P-

partitioned security mode

A mode of operation wherein all personnel have the clearance but not necessarily formal access approval and need-to-know for all information contained in the system. Not to be confused with *compartmented security mode*.

password

A protected/private character string used to authenticate an identity.

penetration

The successful act of bypassing the security mechanisms of a system.

penetration signature

The characteristics or identifying marks that may be produced by a penetration.

penetration study

A study to determine the feasibility and methods for defeating controls of a system.

penetration testing

The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints applied to ordinary users.

periods processing

The processing of various levels of sensitive information at distinctly different times. Under periods processing, the system must be purged of all information from one processing period before transitioning to the next when there are different users with differing authorizations.

permissions

A description of the type of authorized interactions a subject can have with an object. Examples include: read, write, execute, add, modify, and delete.

personnel security

The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances.

physical security

The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

piggyback

Gaining unauthorized access to a system via another user's legitimate connection. See *between-the-lines entry.*

Preferred Products List (PPL)

A list of commercially produced equipments that meet TEMPEST and other requirements prescribed by the National Security Agency. This list is included in the NSA Information Systems Security Products and Services Catalogue, issued quarterly and available through the Government Printing Office.

print suppression

Eliminating the displaying of characters in order to preserve their secrecy; e.g., not displaying the characters of a password as it is keyed at the input terminal.

privileged instructions

A set of instructions (e.g., interrupt handling or special computer instructions) to control features (such as storage protection features) that are generally executable only when the automated system is operating in the executive state.

procedural security

Synonymous with *administrative security.*

process

A program in execution. See *domain and subject.*

protection philosophy

An informal description of the overall design of a system that delineates each of the protection mechanisms employed. A combination, appropriate to the evaluation class, of formal and informal techniques is used to show that the mechanisms are adequate `to enforce the security policy.

protection ring

One of a hierarchy of privileged modes of a system that gives certain access rights to user programs and processes authorized to operate in a given mode.

protection-critical portions of the TCB

Those portions of the TCB whose normal function is to deal with the control of access between subjects and objects. Their correct operation is essential to the protection of the data on the system.

protocols

A set of rules and formats, semantic and syntactic, that permits entities to exchange information.

pseudo-flaw

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

Public Law 100-235 (P.L. 100-235)

Also known as the Computer Security Act of 1987, this law creates a means for establishing minimum acceptable security practices for improving the security and privacy of sensitive information in federal computer systems. This law assigns to the National Institute of Standards and Technology responsibility for developing standards and guidelines for federal computer systems processing unclassified data. The law also requires establishment of security plans by all operators of federal computer systems that contain sensitive information.

purge

The removal of sensitive data from an AIS, AIS storage device, or peripheral device with storage capacity, at the end of a processing period. This action is performed in such a way that there is assurance proportional to the sensitivity of the data that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge. After a purge, the medium can be declassified by observing the review procedures of the respective agency.

-Q-

This document contains no entries beginning with the letter “Q”.

-R-

read

A fundamental operation that results only in the flow of information from an object to a subject.

read access

Permission to read information.

recovery procedures

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

reference monitor concept

An access-control concept that refers to an abstract machine that mediates all accesses to objects by subjects.

reference validation mechanism

An implementation of the reference monitor concept. A security kernel is a type of reference validation mechanism.

reliability

The probability of a given system performing its mission adequately for a specified period of time under the expected operating conditions.

residual risk

The portion of risk that remains after security measures have been applied.

residue

Data left in storage after processing operations are complete, but before degaussing or rewriting has taken place.

resource encapsulation

The process of ensuring that a resource not be directly accessible by a subject, but that it be protected so that the reference monitor can properly mediate accesses to it.

restricted area

Any area to which access is subject to special restrictions or controls for reasons of security or safeguarding of property or material.

risk

The probability that a particular threat will exploit a particular vulnerability of the system.

risk analysis

The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management. Synonymous with *risk assessment.*

risk assessment

Synonymous with *risk analysis.*

risk index

The disparity between the minimum clearance or authorization of system users and the maximum sensitivity (e.g., classification and categories) of data processed by a system. See CSC-STD-003-85 and CSC-STD-004-85 for a complete explanation oft his term.

risk management

The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

-S-

safeguards

See *security safeguards.*

scavenging

Searching through object residue to acquire unauthorized data.

secure configuration management

The set of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of ensuring that changes will not lead to violations of the system's security policy.

secure state

A condition in which no subject can access any object in an unauthorized manner.

secure subsystem

A subsystem that contains its own implementation of the reference monitor concept for those resources it controls. However, the secure subsystem must depend on other controls and the base operating system for the control of subjects and the more primitive system objects.

security critical mechanisms

Those security mechanisms whose correct operation is necessary to ensure that the security policy is enforced.

security evaluation

An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive information. One type, a product evaluation, is an evaluation performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done for the purpose of assessing a system's security safeguards with respect to a specific operational mission and is a major step in the certification and accreditation process.

security fault analysis

A security analysis, usually performed on hardware at gate level, to determine the security properties of a device when a hardware fault is encountered.

security features

The security-relevant functions, mechanisms, and characteristics of system hardware and software. Security features are a subset of system security safeguards.

security filter

A trusted subsystem that enforces a security policy on the data that pass through it.

security flaw

An error of commission or omission in a system that may allow protection mechanisms to be bypassed.

security flow analysis

A security analysis performed on a formal system specification that locates potential flows of information within the system.

security kernel

The hardware, firmware, and software elements of a TCB that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct.

security label

A piece of information that represents the security level of an object.

security level

The combination of a hierarchical classification and a set of nonhierarchical categories that represents the sensitivity of information.

security measures

Elements of software, firmware, hardware, or procedures that are included in a system for the satisfaction of security specifications.

security perimeter

The boundary where security controls are in effect to protect assets.

security policy

The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

security policy model

A formal presentation of the security policy enforced by the system. It must identify the set of rules and practices that regulate how a system manages, protects, and distributes sensitive information. See *Bell-La Padula model* and *formal security policy model.*

security range

The highest and lowest security levels that are permitted in or on a system, system component, subsystem or network.

security requirements

The types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

security requirements baseline

A description of minimum requirements necessary for a system to maintain an acceptable level of security.

security safeguards

The protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards may include but are not necessarily limited to: hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices. Also called safeguards.

security specifications

A detailed description of the safeguards required to protect a system.

security test and evaluation

An examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system.

security testing

A process used to determine that the security features of a system are implemented as designed. This includes hands-on functional testing, penetration testing, and verification.

sensitive information

Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but that has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

sensitivity label

A piece of information that represents the security level of an object. Sensitivity labels are used by the TCB as the basis for mandatory access control decisions.

simple security condition

See *simple security property*.

simple security property

A Bell-La Padula security model rule allowing a subject read access to an object only if the security level of the subject dominates the security level of the object. Synonymous with *simple security condition.*

single-level device

An automated information systems device that is used to process data of a single security level at any one time.

Software Development Methodologies

Methodologies for specifying and verifying design programs for system development. Each methodology is written for a specific computer language. See *Enhanced Hierarchical Development Methodology, Formal Development Methodology, Gypsy Verification Environment* and *Hierarchical Development Methodology*.

software security

General purpose (executive, utility or software development tools) and applications programs or routines that protect data handled by a system.

software system test and evaluation process

A process that plans, develops and documents the quantitative demonstration of the fulfillment of all baseline functional performance, operational and interface requirements.

spoofing

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

stand-alone, shared system

A system that is physically and electrically isolated from all other systems, and is intended to be used by more than one person, either simultaneously (e.g., a system with multiple terminals) or serially, with data belonging to one user remaining available to the system while another user is using the system (e.g., a personal computer with non removable storage media such as a hard disk).

stand-alone, single-user system

A system that is physically and electrically isolated from all other systems, and is intended to be used by one person at a time, with no data belonging to other users remaining in the system (e.g., a personal computer with removable storage media such as a floppy disk).

star property

See **-property, page 2*.

State Delta Verification System

A system designed to give high confidence regarding microcode performance by using formulae that represent isolated states of a computation to check proofs concerning the course of that computation.

state variable

A variable that represents either the state of the system or the state of some system resource.

storage object

An object that supports both read and write accesses.

Subcommittee on Automated Information Systems Security (SAISS)

NSDD-145 authorizes and directs the establishment, under the NTISSC, of a permanent Subcommittee on Automated Information Systems Security. The SAISS is composed of one voting member from each organization represented on the NTISSC.

Subcommittee on Telecommunications Security (STS)

NSDD-145 authorizes and directs the establishment, under the NTISSC, of a permanent Subcommittee on Telecommunications Security. The STS is composed of one voting member from each organization represented on the NTISSC.

subject

An active entity, generally in the form of a person, process, or device, that causes information to flow among objects or changes the system state. Technically, a process/domain pair.

subject security level

A subject's security level is equal to the security level of the objects to which it has both read and write access. A subject's security level must always be dominated by the clearance of the user with which the subject is associated.

supervisor state

Synonymous with *executive state*.

System Development Methodologies

Methodologies developed through software engineering to manage the complexity of system development. Development methodologies include software engineering aids and high-level design analysis tools.

system high security mode

See *modes of operation*.

system integrity

The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

system low

The lowest security level supported by a system at a particular time or in a particular environment.

System Security Officer (550)

See *Information System Security Officer*.

Systems Security Steering Group

The senior government body established by NSDD-145 to provide top-level review and policy guidance for the telecommunications security and automated information systems security activities of the U.S. Government. This group is chaired by the Assistant to the President for National Security Affairs and consists of the Secretary of State, Secretary of Treasury, the Secretary of Defense, the Attorney General, the Director of the Office of Management and Budget, and the Director of Central Intelligence.

-T-

tampering

An unauthorized modification that alters the proper functioning of an equipment or system in a manner that degrades the security or functionality it provides.

technical attack

An attack that can be perpetrated by circumventing or nullifying hardware and software protection mechanisms, rather than by subverting system personnel or other users.

technical vulnerability

A hardware, firmware, communication, or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user, or manager of the system.

TEMPEST

The study and control of spurious electronic signals emitted by electrical equipment.

terminal identification

The means used to uniquely identify a terminal to a system.

threat

Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

threat agent

A method used to exploit a vulnerability in a system, operation, or facility.

threat analysis

The examination of all actions and events that might adversely affect a system or operation.

threat monitoring

The analysis, assessment, and review of audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted violations of system security.

ticket-oriented

A computer protection system in which each subject maintains a list of unforgeable bit patterns, called tickets, one for each object the subject is authorized to access. Compare *list-oriented.*

time-dependent password

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

top-level specification

A nonprocedural description of system behavior at the most abstract level; typically, a functional specification that omits all implementation details.

tranquility

A security model rule stating that the security level of an object cannot change while the object is being processed by an AIS.

trap door

A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. It is activated in some innocent-appearing manner; e.g., a special "random" key sequence at a terminal. Software developers often introduce trap doors in their code to enable them to reenter the system and perform certain functions. Synonymous with *back door*.

Trojan horse

A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security or integrity.

trusted computer system

A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information.

Trusted Computing Base (TCB)

The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to enforce correctly a unified security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance level) related to the security policy.

trusted distribution

A trusted method for distributing the TCB hardware, software, and firmware components, both originals and updates, that provides methods for protecting the TCB from modification during distribution and for detection of any changes to the TCB that may occur.

trusted identification forwarding

An identification method used in networks whereby the sending host can verify that an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host.The receiving host can then verify that the user is validated for access to its system. This operation may be transparent to the user.

trusted path

A mechanism by which a person at a terminal can communicate directly with the TCB. This mechanism can only be activated by the person or the TCB and cannot be imitated by untrusted software.

trusted process

A process whose incorrect or malicious execution is capable of violating system security policy.

trusted software

The software portion of the TCB.

-U-

untrusted process

A process that has not been evaluated or examined for adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms.

user

Person or process accessing an AIS either by direct connections (i.e., via terminals), or indirect connections (i.e., prepare input data or receive output that is not reviewed for content or classification by a responsible individual).

user ID

A unique symbol or character string that is used by a system to identify a specific user.

user profile

Patterns of a user's activity that can be used to detect changes in normal routines.

-V-

verification

The process of comparing two levels of system specification for proper correspondence (e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code). This process may or may not be automated.

virus

A self-propagating Trojan horse, composed of a mission component, a trigger component, and a self-propagating component.

vulnerability

A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security policy.

vulnerability analysis

The systematic examination of systems in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.

vulnerability assessment

A measurement of vulnerability which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack.

-W-

work factor

An estimate of the effort or time needed by a potential penetrator with specified expertise and resources to overcome a protective measure.

write

A fundamental operation that results only in the flow of information from a subject to an object.

write access

Permission to write to an object.

-X,Y,Z-

This document contains no entries beginning with the letters “X,” “Y,” or “Z.”

REFERENCES

Air Force Regulation 700-10, “Information Systems Security,” 15 March 1985.

Army Regulation 380-380, “Automated Systems Security,” 3 March 1985.

Department of Defense Computer Security Center, CSC-STD-002-85, “Department of Defense Password Management Guideline,” 12 April 1985.

Department of Defense Computer Security Center, CSC-STD-003-85, “Computer Security Requirements --Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria to Specific Environments,” 25 June 1985.

Department of Defense Computer Security Center, CSC-STD-004-85, “Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements--Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, “25 June 1985.

Department of Defense Directive 5200.1-R, “Information Security Program Regulation,” June 1986.

Department of Defense Directive 5200.28, “Security Requirements for Automated Information Systems,” 21 March 1988

Department of Defense Directive 5200.28-M, "ADP Security Manual,” January 1973.

Department of Defense Directive 5200.28-STD, “Department of Defense Trusted Computer System Evaluation Criteria,” December 1985.

Department of Defense Directive 5215.1, “Computer Security Evaluation Center,” 25 October 1982.

Department of Defense Directive 5230.25, “Withholding of Unclassified Technical Data from Public Disclosure,” 6 November 1984.

Department of Defense Directive 7040.6, “Internal Control Systems,” 24 March 1982.

Department of Defense Instruction 5215.2, “Computer Security Technical Vulnerability Reporting Program (CSTVRP),” 2 September 1986.

Department of Energy Order 5635.1A, “Control of Classified Documents and Information,” 12 February 1988.

Department of Energy Order 5637.1, “Classified Computer Security Program,” 29 January 1988.

Director of Central Intelligence Directive 1/16, “Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks,” 19 July 1988. (SECRET)

Mitre Corp. Technical Report MTR-8201, “Trusted Computer Systems - Glossary,” March 1981.

National Security Decision Directive 145, “National Policy on Telecommunications and Automated Systems Security,” 17 December 1984.

Office of Navy Operations Instruction 5239.1A, “Department of the Navy Automatic Data Processing Security Program,” 8 March 1982.

Public Law 100-235, “Computer Security Act of 1987,” 8 January 1988. Stein, Jess (ed.), “The Random House Dictionary of the English Language,” Random House, 1982.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION **UNCLASSIFIED**	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT **Unlimited Distribution**
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) **NCSC-TG-004**	5. MONITORING ORGANIZATION REPORT NUMBER(S) **Library No.: S-231,238**
6a. NAME OF PERFORMING ORGANIZATION **National Computer Security Center** 6b. OFFICE SYMBOL *(If applicable)* **C11**	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS *(City, State and ZIP Code)* **ATTN: C11** **9800 Savage Road** **Ft. George G. Meade, MD 20755-6000**	7b. ADDRESS *(City, State and ZIP Code)*
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL *(If applicable)*	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS *(City, State and ZIP Code)*	10. SOURCE OF FUNDING NOS. PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT NO.
11. TITLE *(Include Security Classification)* **Glossary of Computer Security Terms**	

12. PERSONAL AUTHOR(S)
Whittaker, Mary S.; Berg, Sue

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT *(Yr, Mo., Day)*	15. PAGE COUNT
Final	FROM ____ TO ____	**881021**	**58**

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
FIELD	GROUP	SUB. GR.	**NCSC, Public Law 100-235, NSDD 145, Trusted Computing Base (TCB), Trusted Computer System Evaluation Criteria (TCSEC), Orange Book, computer security, risk analysis, vulnerability assessment**

19. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*
Glossary of Computer Security terms chiefly from National Computer Security Center and other official government sources. Terms on a broad range of topics, including risk analysis, vulnerability assessment, and Orange Book.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED	21. ABSTRACT SECURITY CLASSIFICATION **UNCLASSIFIED**
22a. NAME OF RESPONSIBLE INDIVIDUAL **Blaine W. Burnham**	22b. TELEPHONE NUMBER *(Include Area Code)* **(301) 859-4463** 8b. OFFICE SYMBOL **C11**

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

☆ U.S. GOVERNMENT PRINTING OFFICE;1191-520-047/21286