# BY ORDER OF THE SECRETARY OF THE AIR FORCE

# AIR FORCE MANUAL 33-229 1 NOVEMBER 1997



Communications and Information

# CONTROLLED ACCESS PROTECTION (CAP)

**NOTICE:** This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCA/SYS (MSgt Charbonneau)

Supersedes AFSSI 5002, 26 August 1996.

Certified by: HQ USAF/SCXX (Lt Col Webb)
Pages: 14

Distribution: F

Distribution. 1

This manual implements the mandated controlled access protection (CAP) requirements of Air Force Systems Security Instruction (AFSSI) 5102, Computer Security (COMPUSEC) for Operational Systems, as outlined in Department of Defense (DoD) 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985 (referred to as the Orange Book), and the National Telecommunications and Information Systems Security Policy (NTISSP) 200, National Policy on Controlled Access Protection. We encourage the use of extracts. Refer questions and comments on technical contents of this manual through appropriate command channels to Headquarters Air Force Communications Agency (HQ AFCA/GCI), 203 West Losey Street, Room 2040, Scott AFB IL 62225-5234. Refer recommended changes and conflicts between this and other publications to HQ AFCA/XPXP, 203 West Losey Street, Room 1060, Scott AFB IL 62225-5233, on Air Force Form 847, Recommendation for Change of Publication, with an information copy to Headquarters United States Air Force (HQ USAF/SCXX), 1030 Air Force Pentagon, Washington DC 20330-5000.

#### **SUMMARY OF REVISIONS**

This is the initial publication of AFMAN 33-229. It replaces AFSSI 5002, *Controlled Access Protection (CAP)*.

## Section A—General Information

- **1. Purpose.** This manual provides guidance for achieving the mandated computer security (COM-PUSEC) requirements of the C2 criteria class CAP. Within this document, and when discussing CAP, the term "C2" does not stand for "command and control," but indicates "criteria class C2." The Orange Book describes the technical aspects of C2. This manual interprets the Orange Book and assists the designated approving authority (DAA), computer systems manager (CSM), and computer systems security officer (CSSO) in complying with the intent of the C2 criteria class requirements for information systems (IS).
  - 1.1. Glossary of References, Abbreviations, Acronyms, and Terms. See **Attachment 1** and Air Force Manual (AFMAN) 33-270, *Command, Control, Communications, and Computer (C4) Systems Security Glossary*.

- 1.2. Introduction. The thrust of CAP is achieving four C2 criteria class COMPUSEC features. Achieving these requirements as mandated in NTISSP 200 provides a minimum protection and is an alternative for formal evaluation rating from the National Computer Security Center (NCSC) on legacy ISs. To provide an appropriate level of protection in the operational legacy ISs, implement the Orange Book C2 criteria class in a cost-effective, feasible manner. The Orange Book criteria were written at a technical level for an intended audience of COMPUSEC professionals developing a trusted computing base (TCB) system, and therefore require Air Force interpretation and explanation for legacy ISs. This manual addresses the interpretations applicable to all ISs and more stringent requirement adherence on certain ISs for full C2 criteria class. Unlike a formal technical NCSC evaluation, non-technical safeguards with controls (physical, procedural, administrative, etc.) provide the criteria to achieve C2 criteria class requirements for legacy ISs known as "C2 functionality," or "CAP."
- 1.3. CAP Functionality. The CAP requirements in NTISSP 200 consist of identification and authentication (I&A), discretionary access control (DAC), audit, and object reuse. The achievement of all four requirements through automated, procedural, or administrative means meets CAP requirements in NTISSP 200. This may include the assurance control objective requirements (architecture and testing), or the documentation requirements (Security Features User's Guide [SFUG] and Trusted Facility Manual [TFM]) from the Orange Book. Subsequent sections explain the goal of each CAP featured.
  - 1.3.1. This manual provides instructions for assessment of CAP feature requirements. The DAA has the latitude to decide exactly how the implementation of security requirements achieve CAP.
  - 1.3.2. Address all of the CAP requirements in the IS certification and accreditation (C&A) documentation.
  - 1.3.3. To facilitate achievement of the C2 criteria class requirements, this manual separates the four CAP security features into sections, outlines implementation, and outlines mitigating considerations.

## 1.4. Objectives.

- 1.4.1. Primary objectives are:
  - 1.4.1.1. Identify CAP requirements for given modes of operation and levels of sensitivity.
  - 1.4.1.2. Interpret the CAP requirements for operational ISs not formally evaluated by the NCSC.
  - 1.4.1.3. Provide alternative safeguards for meeting the intent of the mandated CAP when the NCSC has not evaluated the IS for C2 criteria class compliance.
- 1.4.2. Secondary objectives are to provide for consideration in:
  - 1.4.2.1. Determining applicable Air Force ISs.
  - 1.4.2.2. Determining the need for full or partial compliance through technical or non-technical means depending on the IS mode of operation.
  - 1.4.2.3. Understanding CAP requirements.
  - 1.4.2.4. Identifying mitigating actions to compensate for security features that are not built-in at time of acquisition, development, or manufacture.
  - 1.4.2.5. Suggesting, where possible, safeguards to mitigate CAP requirements that are unob-

tainable or not feasible from an economic standpoint.

- 1.5. Applicability. This manual applies to all Air Force ISs except exclusions as noted. Newly acquired ISs will meet full C2 criteria class (the Orange Book) upon responsibility transfer to the operations phase. Therefore, the focus of this manual is the noncompliant legacy ISs.
- 1.6. Relationship to Other Publications. This publication provides the guidance for determining CAP requirements and assessing compliance of operational ISs as specified by NTISSP 200 and DoD Directive (DoDD) 5200.28, Security Requirements for Automated Information Systems (AISs), March 21, 1988. NTISSP 200 is a national policy released by the National Telecommunications and Information Systems Security Council (NTISSC) in 1987. DoDD 5200.28 includes the DoD approach to achieving the NTISSP 200 requirement. AFSSI 5102 serves as an Air Force IS umbrella document covering COMPUSEC to include procedures and guidance. AFSSI 5102 requires C2 compliance for all Air Force ISs and points to this manual for implementation guidance.
- 1.7. Description of C2 Criteria Class. The following is a description of C2 (CAP criteria) extracted from the Orange Book for a division and class of C2. "Systems in this class enforce a more finely grained discretionary access control than (C1) systems, making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation." The following are minimal requirements for systems assigned a class C2 rating:
  - 1.7.1. Security Policy: DAC and object reuse.
  - 1.7.2. Accountability: I&A and audit.
  - 1.7.3. Assurance: IS architecture, IS integrity, security testing.
  - 1.7.4. Documentation: SFUG, TFM, and test/design documentation.
- 1.8. CAP Security Features. The C2 criteria class requirements in **Table 1.** further describe the minimum security requirements of the four CAP features for a specific mode of operation. ISs operated in the dedicated mode generally do not need to meet all CAP requirements. However, even in dedicated mode, the Air Force strongly encourages you to use all obtainable or available features. See AFSSI 5102, Attachment 4, for a more detailed explanation of the security modes of operation.

Table 1. C2 Criteria Class Requirements.

	CAP Minimum Feature Requirements (See Note)			
Mode of Operation	Identification & Authentication	Audit	Discretionary Access Control	<b>Object Reuse</b>
Dedicated (Stand-alone Information System)	DAA determines	DAA deter- mines		
Dedicated	X	X	DAA deter- mines	X (functional)
System High (Sensitive Information)	X	X	X (functional)	X (functional)
System High Classified	X	X	X	X

#### **NOTE:**

An "X" indicates the requirement MUST be present; an "X (functional)" indicates the requirement must be present or procedurally mitigated. In either case, address the security requirement during the C&A. The DAA must approve any variance or waiver when a requirement is not technically possible or economically feasible.

1.9. DAA Responsibilities. The ISs DAA, with assistance from the appropriate CSSO, determines the applicability and maintenance of CAP throughout the IS life cycle. The DAA is responsible for approving any other applied safeguards (physical, administrative, etc.) and commercial add-on subsystem packages when the IS does not inherently provide the four CAP features. For Air Force purposes, the use of DAA-approved safeguards will satisfy the CAP requirement.

## Section B—Controlled Access Protection Requirement - Identification and Authentication

- **2. Introduction.** Discretionary and mandatory access controls rely on the ISs' ability to verify user identity prior to beginning a processing session. User identification is the process by which individuals identify themselves to the system as a valid user. Two other CAP requirements (DAC and audit) depend on the ability to grant privileges and track actions to a single user that is dependably identified. Authentication is the procedure by which the system verifies they are indeed the user, and have a right to use the system.
  - 2.1. Requirement. All ISs must have user accountability based on the requirements levied by Public Law 100-235, *Computer Security Act of 1987*; NTISSP 200; DoDD 5200.28; AFSSI 5102; and AFSSI 5013, *Identification and Authentication* (will convert to AFMAN 33-223). You must fully test and document I&A during the C&A process. The actual technical description of I&A is: "The TCB (system) shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual AIS user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by the individual." (Reference: DoD 5200.28-STD)

- 2.2. Interpretation. The major criteria of I&A is individual user accountability of access to an IS and its information. This requirement entails user unique identification with some form of authentication. Upon individual user identification input, the IS locates the authorization or I&A file. Authentication provides verification of a user's identity. Without authentication the individual user identification has no credibility. Additionally, the IS must protect the authentication file (e.g., password file) to limit read or write access to only system administrators or the CSM.
- 2.3. Implementation. The most common method of providing the required I&A feature is by using user IDs (identification) and passwords (authentication), but that is by no means the strongest. The use of one-time passwords is encouraged, particularly where clear-text passwords are sent over a non-trusted path or medium (e.g., the Internet). There are "smart" cards with embedded chip sets that contain identification information with challenge and response algorithms for authentication purposes. Also, smart card add-on subsystem software packages may offer a means to provide positive I&A without the disadvantages of having to manage user IDs and passwords. In addition, industry add-on packages use new biometrics technology such as retina scanners, fingerprint readers, etc. I&A features must meet the requirements outlined in AFSSI 5013. For technical level implementation of I&A refer to NCSC-TG-017, A Guide to Understanding Identification and Authentication in Trusted Systems.
- 2.4. Network Considerations. I&A is crucial in maintaining the integrity of Air Force network information infrastructure. The DAA needs to discourage the establishment and use of accounts that do not provide individual access control to an IS for accountability (e.g., the use of group IDs or group passwords). The DAA must specifically approve "Guest" accounts and anonymous file transfer protocol (FTP). Further network considerations on I&A requirements are in AFSSI 5013. For technical level implementation refer to NCSC-TG-005, *Trusted Network Interpretation*, Section 2.2.
- 2.5. Mitigation of Unobtainable I&A Elements. The use of a system level basic input/output system (BIOS) password will authenticate a single user of a stand-alone IS. Strong physical security with controls to IS access partially mitigates the absence of I&A elements. In the case of IS server limitations, the sharing of passwords partially mitigates the absence of I&A.

## Section C—Controlled Access Protection Requirement - Discretionary Access Control

- **3. Introduction.** DAC provides the ability to control a user's access to information according to the authorization granted the user. Unlike mandatory access control (MAC) which is implemented by the IS, the individual user administers DAC.
  - 3.1. Requirement. All Air Force shared (i.e., multi-user) ISs must have DAC based on the requirements levied by Public Law 100-235, NTISSP 200, DoDD 5200.28, and AFSSI 5102. The actual technical description of DAC is: "The TCB (system) shall define and control access between named objects (e.g., files, and programs) in the AIS. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined group of individuals, or both, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or default, provide that objects are protected from authorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users." (Reference: DoD 5200.28-STD)

- 3.2. Interpretation. DAC provides the data owner (individual user or groups) a capability to specify permissions (read, write, delete, or execute the directories and files) to information for each of their IS objects (e.g., files, programs) on fixed media, removable media, memory storage, etc. To achieve DAC, measures are required to provide the ISs' functional office of primary responsibility, system administrator, and users with the ability to control access to their data files and programs. The DAC specifies access permission for either individuals, groups of individuals, or both. The DAC feature, together with the I&A feature, control all user access privileges. For more technical information concerning full implementation of DAC refer to NCSC-TG-003, *A Guide to Understanding Discretionary Access Control in Trusted Systems*.
- 3.3. Implementation. Ensure activation of all available IS access control features and consider the use of DAC add-on subsystem (i.e., commercial off-the-shelf [COTS] software/firmware packages).
- 3.4. Network Considerations. The DAA should consider the use of DAC add-on subsystem (i.e., COTS software/firmware packages) for *DOS/Windows* in both network and stand-alone mode. Additionally, where technically possible, partitioning networked information in separate servers (grouped by need to know) in a *DOS/Windows* server environment controls file access. For example, an IS (file server) containing sensitive information could be partitioned for access by authorized individual users, groups of users, or users in a specific domain. Effective and efficient local area network (LAN) administration will naturally achieve a measure of DAC. For technical-level implementation refer to NCSC-TG-005, Section 2.2.
- 3.5. Mitigating Unobtainable DAC Elements. The Air Force recognizes that many operational ISs acquired or developed before the establishment and promulgation of the Orange Book cannot fully satisfy the DAC requirement. An example is a *DOS/Windows* desktop personal computer (PC) that does not provide a DAC control for "read" access to the hard drive. In *DOS/Windows* systems, the creation or modification of a file to be "read only" is an implementation of DAC, albeit a very weak one. However, there are several ways to partially satisfy and implement the DAC feature requirements. Enforce the use of the available and applicable access controls (e.g., "read-only") when other means are not economically feasible. If a DAC feature is not inherent in the IS, place sensitive (classified or unclassified) information on removable media and use physical, administrative, and procedural controls. Using the IS hard drive instead of common or shared drives for sensitive information also mitigates the absence of DAC.

# Section D—Controlled Access Protection Requirement - Audit

- **4. Introduction.** To achieve CAP, the IS must have dependable audit capabilities for security relevant events. That is, a TCB (system) provides the ability for authorized personnel to audit any action that may potentially cause access to, generation of, or effect the release of sensitive information. Selectively acquire and base audit data on the auditing needs of a particular installation and, or application. Sufficient audit data is required to support tracing events to a specific individual who has taken the actions or on whose behalf the actions were taken.
  - 4.1. Requirement. All Air Force shared ISs must have an audit capability based on the requirements levied by Public Law 100-235, NTISSP 200, DoDD 5200.28, and AFSSI 5102. The actual technical description of audit is: "The TCB (system) shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized

for the audit data. The TCB shall be able to record the following types of events: use of the I&A mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, actions taken by computer operators and system administrators and system officers, and other security related events. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For I&A events the origin of the request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The AIS administrator shall be able to selectively audit the actions of any one or more users based on individual identity." (Reference: DoD 5200.28-STD)

- 4.2. Interpretation. The audit requirement is that the IS has the capability to collect information regarding IS events, thus supporting the monitoring of IS use and the investigation of possible attempts to breach security. DAAs and CSSOs must determine what events the IS must audit and any additional mission-specific audit requirements. The audit mechanism must record, examine, and review security-relevant activities (i.e., date/time of user logon/logoff, object creation, deletion, modification, unsuccessful logon attempts, and attempts to access protected [audit or password] files, etc.), either as they are occurring or in retrospect. The capability to perform real-time auditing is beyond the requirements of CAP. However, the capability must exist to (a) configure the IS to audit a set of events determined by the CSSO, (b) present audit information in a manner useful in investigating security incidents, and (c) monitor users' actions in order to anticipate and potentially neutralize impending security attacks.
- 4.3. Implementation. For more technical information concerning full implementation of auditing refer to NCSC-TG-001, *A Guide to Understanding Audit in Trusted Systems*.
  - 4.3.1. Provide a mechanism for recording:
    - 4.3.1.1. User I&A mechanisms.
    - 4.3.1.2. User actions to open, close, create, execute, modify, or delete programs or files.
  - 4.3.2. For each auditable event, the audit mechanism must record the following information:
    - 4.3.2.1. Date and time of the event.
    - 4.3.2.2. Type of event
    - 4.3.2.3. Success or failure of the event.
    - 4.3.2.4. Name of program or file introduced, accessed, modified, or deleted.
  - 4.3.3. To provide security personnel the ability to research past events related to a current IS irregularity or security incident, retain audit trails for a reasonable period of time (e.g., 3 months). Once determined, specify the retention period for audit trails in the system's security policy. Audit trails will aid in reconstruction of past IS events, determination of their impact, and identification of related unauthorized access or use of IS resources and data.
- 4.4. Network Considerations.
  - 4.4.1. In addition to the implementation requirements from paragraph 4.3, networks must provide a mechanism for recording the following events:
    - 4.4.1.1. Actions taken by IS operators, system administrators, and system security administrators (e.g., adding a user).

- 4.4.1.2. Any event that attempts to change the security profile of the IS (e.g., change access controls, change the security level of the subject, or change user password).
- 4.4.1.3. Any event that attempts to violate the system security policy of the IS (e.g., too many attempts to log in, attempts to violate the access control limits of a device, and attempts to downgrade a file).
- 4.4.1.4. Changes in users' privileges or identification.
- 4.4.1.5. Remote access activity such as account name (UserId) and point of origin (IS identification).
- 4.4.2. In addition to the implementation requirements above, networks must record the following information for each auditable event:
  - 4.4.2.1. The unique identifier of the user or device generating events.
  - 4.4.2.2. Origin of the request for I&A events.
- 4.5. Mitigation of Unobtainable Audit Elements.
  - 4.5.1. To mitigate the lack of any required audit element, the CSSO and the CSM, with DAA approval, may choose to reduce the risk through employing physical, procedural, and administrative safeguards as a countermeasure.
  - 4.5.2. Limiting physical access for a given PC to a specific individual or group provides a degree of audit in that all actions taken on the IS are attributable to that individual or group. Selective IS audit events must identify user violations of the security policies (unsuccessful logon attempts, attempts to violate the DAC features, unauthorized attempts to access or modify the audit files, etc.)
  - 4.5.3. For stand-alone ISs processing classified, you must maintain a manual log of user activity and list procedures in the C&A documentation.
  - 4.5.4. Automated intrusion detection software and the Automated Security Incident Measurement Program are elements that partially implement or mitigate the audit requirement.
  - 4.5.5. Although the audit requirements are certainly not built in to *DOS/Windows* IS, if only one person uses an IS, or if one person at a time uses an IS and annotates IS usage on a manual log, then all security relevant actions are traceable to that user.
  - 4.5.6. BIOS passwords and keyboard/system locks limit IS access to authorized users and aid in auditing because only a small number of individuals have the necessary "key."
  - 4.5.7. Strong physical controls and strong I&A mechanisms can make up for an a lack of audit features built into an IS.
  - 4.5.8. Knowledge or documentation of who used an IS along with the simple date-time stamp disk operating system (DOS) place on files does provide a crude audit capability. It is unlikely that a development effort to create a robust audit capability is feasible in legacy ISs. DAAs may consider add-on (COTS) software that is readily available that provides audit in *DOS/Windows* systems.
  - 4.5.9. Network Mitigating Considerations. Do not disable the audit function in network software. Do not make the audit function so intensive or granular that it significantly degrades IS perfor-

mance. Network administrators and IS security personnel must develop and implement an audit review process based on mission traffic and sensitivity. Log relevant events in an audit log and retain for a carefully considered period of time. Again, in networks, to mitigate the lack of this element, with DAA approval, the CSSO and the CSM may choose to reduce the risk through employing other physical, procedural, and administrative safeguards as a countermeasure.

## Section E—Controlled Access Protection Requirement - Object Reuse

- **5. Introduction.** The intent of object reuse is to prevent inadvertent disclosure of information to unauthorized users. In contrast with DAC, which seeks to protect the containers of information (i.e., objects), the object reuse requirement seeks to protect the information contained in the ISs storage objects (e.g., primary storage, fixed media, removable media, etc.) Thus object reuse requires initializing of each container (cleared) before it is allocated/reallocated to a user or process. See AFSSI 5020, *Remanence Security* (will convert to AFMAN 33-224) for a more detailed discussion of the object reuse.
  - 5.1. Requirement. All shared ISs must have object reuse capabilities based on the requirements levied by Public Law 100-235, NTISSP 200, DoDD 5200.28, and AFSSI 5102. Also, NCSC-TG-005, Section 2.2 lists audit requirements and considerations in network environments. The actual technical description of object reuse is: "All authorizations to the information contained within a storage object shall be revoked prior to the initial assignment, allocation, or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object that has been released back to the system." (Reference: DoD 5200.28-STD)
  - 5.2. Implementation. For more technical information concerning full implementation of object reuse, refer to NCSC-TG-018, A Guide to Understanding Object Reuse in Trusted Systems. To achieve object reuse, completely erase or overwrite each available storage media location before reassignment to another user. This includes unassigned storage areas (disk), and storage locations turned over to the IS for reallocation to a user. The deletion of assignment "pointers" in the allocation tables does not meet this requirement. Encryption of the data files or program locations does not comply with this requirement.
    - 5.2.1. In operational *DOS/Windows* desktop ISs, implement add-on software packages that have tested and evaluated object reuse features listed in the Evaluated Products Listing (distributed by the National Security Agency [NSA]) or Assessed Products Listing (distributed by HQ AFCA/SYS).
    - 5.2.2. As a procedural means of implementing object reuse, you may develop an instruction or policy to purge unused areas with an evaluated disk wipe software. These programs overwrite (clear) unassigned memory locations at the end of a user session. This procedure should include the removal of power from ISs with volatile memory. For ISs with removable media, use the NSA-approved degaussing equipment (listed in the Degausser Products List) on the media before allowing reuse by another user facilitates this process. AFSSI 5020 contains Air Force policy on magnetic remanence and object reuse.
    - 5.2.3. There are several operating system upgrades available that are suitable for use in achieving object reuse.

- 5.3. Network Mitigating Considerations. NCSC-TG-005, Section 2.2 lists object reuse requirements in network environments. It is important that the object reuse inherent in UNIX-based servers is not intentionally defeated to allow for data recovery. System administrators must not develop or implement procedures to write files to a temporary directory prior to the "remove" command. In *DOS/Windows* servers, as a minimum, develop and implement a procedure to "wipe" or clear file and mailbox areas when you delete or remove users from a network or server. A carefully administered policy of clearing files and mail areas used by departing personnel will mitigate the absence of object reuse.
- 5.4. Mitigating Unobtainable Object Reuse Elements. Many current COTS ISs that were acquired or developed before the establishment and promulgation of the DoD 5200.28-STD cannot fully satisfy the object reuse requirement; it is the most difficult of the CAP requirements to obtain in *DOS/Windows*-based networked PCs. To achieve "functional" object reuse, "defragging" routines must achieve a degree of object reuse in disk storage. Defragmentation, while not required, rewrites over all storage locations (used and unused) to eliminate any "fragmenting" of files and programs on disks to increase input/output efficiency. Frequent defragmenting eliminates much of the extraneous data normally available for scavenging.

WILLIAM J. DONAHUE, Lt General, USAF Director, Communications and Information

#### Attachment 1

# GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

#### References

Public Law 100-235, Computer Security Act of 1987

DoDD 5200.28, Security Requirements for Automated Information Systems (AISs), March 21, 1988

DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985 (referred to as the Orange Book)

NTISSP 200, National Policy on Controlled Access Protection

NCSC-TG-001, A Guide to Understanding Audit in Trusted Systems

NCSC-TG-003, A Guide to Understanding Discretionary Access Control in Trusted Systems

NCSC-TG-005, Trusted Network Interpretation

NCSC-TG-017, A Guide to Understanding Identification and Authentication in Trusted Systems

NCSC-TG-018, A Guide to Understanding Object Reuse in Trusted Systems

AFMAN 33-270, Command, Control, Communications, and Computer (C4) Systems Security Glossary

AFSSI 5013, *Identification and Authentication* (to become AFMAN 33-223)

AFSSI 5020, Remanence Security (to become AFMAN 33-224)

AFSSI 5102, Computer Security (COMPUSEC) Program for Operational Systems

#### Abbreviations and Acronyms

**AFSSI**—Air Force Systems Security Instruction

**AIS**—Automated Information System

**BIOS**—Basic Input/Output System

C2—A Division and Class of DoD 5200.28-STD (Orange Book)

**C&A**—Certification and Accreditation

**CAP**—Controlled Access Protection

**COMPUSEC**—Computer Security

**COTS**—Commercial Off-The-Shelf

**CSM**—Computer Systems Manager

**CSSO**—Computer Systems Security Officer

**DAA**—Designated Approving Authority

**DAC**—Discretionary Access Control

**DoD**—Department of Defense

**DoDD**—Department of Defense Directive

**DOS**—Disk Operating System

**EPL**—Evaluated Products List

**FTP**—File Transfer Protocol

**HQ AFCA**—Headquarters Air Force Communications Agency

**HQ USAF**—Headquarters United States Air Force

**I&A**—Identification & Authentication

**IS**—Information System

LAN—Local Area Network

MAC—Mandatory Access Control

NCSC—National Computer Security Center

**NSA**—National Security Agency

NTISSC—National Telecommunications and Information Systems Security Council

NTISSP—National Telecommunications and Information Systems Security Policy

**PC**—Personal Computer

**SFUG**—Security Features User's Guide

**TCB**—Trusted Computing Base

**TFM**—Trusted Facility Manual

#### **Terms**

Accreditation—1. In computer modeling and simulation, an official determination that a model or simulation is acceptable for a specific purpose. (See configuration management, independent review, validation, and verification.) 2. Official management authorization to operate an information system (IS). It is the formal declaration by the designated approving authority that an IS gains approval to operate in a particular security mode using a prescribed set of safeguards and controls.

**Audit**—Independent review and examination of records and activities to assess the adequacy of system controls; to ensure compliance with established policies and operational procedures; and to recommend necessary changes in controls, policies, or procedures.

**Authentication**—A security measure designed to protect a communications system against acceptance of a fraudulent transmission of simulation by establishing the validity of a transmission, message, or originator.

Automated Information System (AIS)—1. A combination of information, computer, and telecommunications resources and other information technology and personnel resources that collect, record, process, store, communicate, retrieve, and display information. 2. Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data, and includes any assembly of software, firmware, and hardware. **NOTE:** The term

"AIS" includes stand-alone systems, communications systems, and computer network systems of all sizes, whether digital, analog, or hybrid; associated peripheral devices and software; process control computers; security components; embedded computer systems; communications switching computers; personal computers; workstations; microcomputers; intelligent terminals; word processors; automated data processing systems; and office automation systems, as may be developed.

Certification—1. The process by which an information system is evaluated for satisfaction of requirements for interoperability, compatibility, and integration. 2. The comprehensive analysis of both the technical and nontechnical security features and countermeasures of an information system to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Computer Systems Manager (CSM)—Official with supervisory or management responsibility for an organization, activity, or functional area that owns or operates an automated information system (includes computers, word processing systems, networks, etc.).

Computer Systems Security Officer (CSSO)—Official who manages the computer security program for an automated information system (AIS)(includes computers, word processing systems, networks, etc.) assigned to them by the computer systems manager; monitors AIS activities; and ensures that the operation, maintenance, and disposal of AIS is according to security policies and practices.

Configuration Management—In computer modeling and simulation, a discipline applying technical and administrative oversight and control to identify and document the functional requirements and capabilities of a model or simulation and its supporting data bases, control changes to those capabilities, and document and report the changes. (See accreditation, independent review, validation, and verification.)

**Designated Approving Authority (DAA)**—Official who formally assumes responsibility for the operation of the system within a specified environment.

**Discretionary Access Control (DAC)**—Means of restricting access to objects based on the identity and need-to-know of users and or groups to which the object belongs. **NOTE:** Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) on to any other subject.

Embedded Computer System—1. A computer system that is integral to a larger system whose primary purpose is not computational. An embedded computer would require major modifications be used for general-purpose computing and is managed as a component of the system in which it is embedded. 2. An automated information system that is preprogrammed to perform or control one or more dedicated function, either in whole or in part, as an integral element of a larger system (i.e., aircraft, missile, ground support equipment, etc.) and, when operational, cannot be modified. Examples of embedded computers are aircraft avionics systems, patient monitoring equipment, and cryptographic equipment.

**Identification**—Process that enables recognition of an entity by an information system. **NOTE:** Unique machine-readable user names generally accomplish this.

**Information System**—Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching interchange, transmission, or reception, of voice and/or data, and includes software, firmware, and hardware. **NOTE:** This term is used interchangeably with automated information systems throughout this document.

**Mechanism**—Functional feature of an automated information system designed to enforce the system security policy and accountability objectives. Examples include passwords and access control lists.

**Object Reuse**—Reassignment of a storage medium (e.g., page frame, disk sector, and magnetic tape) that contained one or more objects, after making sure no residual data remained on the storage medium.

**Safeguards**—Security disciplines (e.g., administrative, procedural, physical, personnel, communications, emanations, and computer security) used in concert to provide the requisite level of protection.

**Security Features**—Security-relevant functions, mechanisms, and characteristics of automated information systems hardware and software (e.g., identification, authentication, audit, and access control).

**Stand-alone Automated Information System**—An AIS that is physically and electrically isolated from all other systems and is intended for use 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).

**Trusted Computing Base (TCB)**—Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. **NOTE:** The ability of a TCB to correctly enforce a unified security policy depends on the correctness of the mechanisms within the TCB, the protection of those mechanisms to ensure their correctness, and the correct input of parameters related to the security policy.

Validation—1. A process normally associated with the collection of intelligence that provides official status to an identified requirement and confirms that the requirement is appropriate for a given collector and has not been previously satisfied. 2. In computer modeling and simulation, the process of determining the degree to which a model or simulation is an accurate representation of the real world from the perspective of the intended uses of the model or simulation. (See accreditation, configuration management, independent review, and verification.)

**Verification**—1. In arms control, any action, including inspection, detection, and identification, taken to ascertain compliance with agreed measures. 2. In computer modeling and simulation, the process of determining that a model or simulation implementation accurately represents the developer's conceptual description and specifications. (See accreditation, configuration management, independent review, and validation.)