



# **CONTROLLED ACCESS PROTECTION (CAP) GUIDEBOOK**

## **MODULE 15**

INFORMATION SYSTEMS SECURITY  
(INFOSEC)  
PROGRAM GUIDELINES

0515-LP-208-8286

Distribution: Submit requests for placement on distribution (including supporting justification), or amendment to the existing distribution, to:

Commanding Officer  
Naval Command, Control and Ocean Surveillance Center  
ISE East Coast Division  
Code 422  
3801 Nebraska Avenue, N.W.  
Washington, DC 20393-5270

Commercial (202) 764-0753  
DSN 764-0753  
E-Mail: [subscribe@infosec.nosc.mil](mailto:subscribe@infosec.nosc.mil)

Electronic versions of this document may be downloaded via  
anonymous ftp from [infosec.nosc.mil](ftp://infosec.nosc.mil) or [//http//infosec.nosc.mil/](http://infosec.nosc.mil/inf.html) [inf.html](http://infosec.nosc.mil/inf.html).

Stocked: Additional copies of NAVSO P-5239-15 can be obtained from the  
Navy Aviation Supply Office (Code 03415), 5801 Tabor Avenue, Philadelphia  
PA 18120-5099, through normal supply channels in accordance with NPFC PUB  
2002D, NAVSUP P-437 or NAVSUP P-485, using AUTODIN, DAMES, or  
MILSTRIP message format to DAAS, Dayton, OH.

Cite stock number 0515-LP-208-8286.

Local reproduction is authorized.

DEPARTMENT OF THE NAVY  
NAVAL INFORMATION SYSTEMS MANAGEMENT CENTER  
ARLINGTON, VA 22202-4311

NAVSO P-5239-15  
DECEMBER 1994

**FOREWORD**

Navy Staff Office Publication (NAVSO Pub) 5239, "Information Systems Security (INFOSEC) Program Guidelines" is issued by the Naval Information Systems Management Center. It consists of a series of modules providing procedural, technical, administrative and/or supplemental guidance for all information systems, whether business or tactical, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or receipt of data. Each module will focus on a distinct program element and describe a standard methodology for planning, implementing and executing that element of the INFOSEC program within the Department of the Navy (DON).

This module, "Controlled Access Protection (CAP) Guidebook", provides the Information Systems Security Manager (ISSM) with guidance and procedures to be used for CAP implementation. CAP describes the minimum set of automated controls that should be provided to DON Automated Information Systems (AISs); and, it provides the DON interpretation of the "Class C2" features/functionality requirement of DODD 5200.28 and SECNAVINST 5239.2.

The guidance contained herein applies to all DON AIS's and is effective upon receipt.

J. G. HEKMAN  
Rear Admiral, SC, USN

NAVSO P-5239-15  
DECEMBER 1994

THIS PAGE INTENTIONALLY BLANK

## TABLE OF CONTENTS

Topic	Page
1. Purpose.....	1
2. Scope.....	1
3. Definitions.....	2
a. Controlled Access Protection (CAP).....	2
b. "Class C2".....	2
c. Information Sensitivity.....	2
d. Security Modes of Operation.....	3
(1) Dedicated Security Mode.....	3
(2) System High Security Mode.....	3
(3) Multilevel Security Mode.....	3
4. CAP Requirement.....	3
a. Background.....	3
b. CAP Controls.....	4
c. "Class C2" Criteria.....	4
d. Summary.....	5
5. CAP Waiver Criteria.....	6
a. Authority.....	6
b. Alternative Protection Requirements.....	6
c. Limitations.....	7
d. Triennial Waiver Review.....	7
e. Submission of Waiver Requests.....	7

- 6. CAP Assessment.....8
  - a. Types of Assessments.....9
    - (1) Basic Assessment.....9
    - (2) Detailed Assessment.....9
    - (3) Recognized-Authority Assessment.....9
  - b. Assessment Considerations..... 10
  - c. Security Mode Determination.....11
    - (1) Dedicated Security Mode AISs.....11
    - (2) System High Security Mode AISs.....11
    - (3) Multilevel Security Mode AISs.....12
  - d. Inherent AIS Assessment Risk.....12
  - e. Assessment Selection Guide..... 13
  
- APPENDIX A TECHNICAL CONSIDERATIONS FOR CONTROLLED ACCESS PROTECTION (CAP) FEATURE IMPLEMENTATION.....A - 1
  
- APPENDIX B CONTROLLED ACCESS PROTECTION (CAP) WAIVER APPROVING AUTHORITIES (WAAs).....B - 1
  
- APPENDIX C EXAMPLE CAP SECURITY MODE ANALYSIS.....C - 1

**DEPARTMENT OF THE NAVY  
CONTROLLED ACCESS PROTECTION (CAP) GUIDEBOOK**

- Ref: (a) DODD 5200.28, Security Requirements for Automated Information Systems (AIS)  
(b) SECNAVINST 5239.2, Department of the Navy Automated Information Systems (AIS) Security Program  
(c) DOD 5200.28-STD, Trusted Computer Security Evaluation Criteria  
(d) NCSC-TG-018, A Guide to Understanding Object Reuse in Trusted Systems  
(e) NCSC-TG-005, Trusted Network Interpretation  
(f) NCSC-TG-021, Trusted Database Interpretation  
(g) FIPS PUB 102, Guideline for Computer Security Certification and Accreditation  
(h) NCSC-TG-028, Assessing Controlled Access Protection  
(i) NAVSO P-5239-10, Department of the Navy Information Systems Security Guidelines, Assessed Products List  
(j) NCSC-TG-009 Version-1, Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria

1. **Purpose.** This document provides guidance and procedures for implementing Controlled Access Protection (CAP) in Department of the Navy (DON) Automated Information Systems (AISs). References (a) and (b) require implementation of "Class C2" features/functionality for all AISs processing General Service (GENSER) classified or unclassified but sensitive information. The DON implements "Class C2" through the CAP requirement.

2. **Scope.** The CAP requirement applies to all DON AISs processing GENSER classified or unclassified but sensitive information whether operational, under development, or in the acquisition pipeline. AISs that are accredited outside of the DON, like the ones operated under the purview of Office of Naval Intelligence (Code 54) will comply with their respective CAP security requirements. *This guideline applies to all platforms (e.g., tactical or mission support stand-alone microcomputers, Local Area Networks (LANs), minicomputer systems, mainframe systems, or any other type of networked AISs. Systems (or subcomponents) operated in the dedicated security mode do not require CAP controls but will require physical, personnel, and administrative security protections.*

3. **Definitions.** The following terms are essential to understanding CAP concepts.

a. **Controlled Access Protection (CAP).** A term which describes the minimum set of automated controls that should be provided to DON AISs. These are: discretionary access control (DAC), user identification and authentication (I&A), auditing of security-relevant events, and clearing of memory and storage before reuse. **CAP applies to a system** and shall be implemented to enforce the system-specific information protection policy. The level of assurance associated with the implementation shall correspond to the local risk. *CAP controls are not physical, personnel, or administrative access controls.* Appendix (A) describes CAP features in detail.

b. **"Class C2"**. A set of criteria for evaluating the security features and level of assurance provided by a product as defined in reference (c). The criteria do not specify or address how to implement the required security features to support system-specific information protection policies. **"Class C2" applies to products**, both commercially-available products (e.g., operating systems, database management systems, and the like) and custom-developed software, firmware and hardware products.

c. **Information Sensitivity.**

(1) Sensitivity of unclassified information shall be determined in accordance with applicable information protection policies (such as those associated with financial, and contractual information, the Privacy Act of 1974, etc.) regarding information sensitivity and requirements for the information's control.

The impact of both unauthorized disclosure and modification shall be considered when determining information sensitivity. *For example, policy treats medically privileged information as highly sensitive to unauthorized disclosure and/or modification but routine administrative or office correspondence information as having a relatively low sensitivity to unauthorized disclosure and/or modification.*

(2) The effect of data aggregation and inference shall be considered when determining the sensitivity of information. Information such as names, addressees, and medical test results, that when considered separately, may have a relatively low sensitivity become significantly more sensitive to unauthorized disclosure when considered collectively. This effect shall be considered in the process of choosing an appropriate assessment alternative (see Section 6).

d. **Security Modes of Operation.** There are inherent risks to the integrity, confidentiality, and availability of information in multi-user computing environments. This occurs when some, but not all, information and/or system capabilities are shared by the users. These risks also vary with the security mode in which an AIS operates. Most DON AISs operate in one of the following security modes:

(1) **Dedicated Security Mode.** All the users of an AIS possess the proper security clearance and have need-to-know for accessing all data processed and stored by the AIS. AISs containing unclassified, unclassified but sensitive, or classified information, can operate in the dedicated mode. All information is handled at the highest classification processed by the system.

(2) **System High Security Mode.** All the users of an AIS possess the proper security clearance, but do not necessarily have a need-to-know for accessing all data processed and stored by the AIS. AISs containing unclassified, unclassified but sensitive, or classified information, can operate in the system high mode. All information is handled at the highest classification processed by the system.

(3) **Multilevel Security Mode.** One or more of the users of an AIS do not possess the proper security clearance for accessing the most sensitive classified data processed and stored by the AIS. The AIS is capable of limiting, in a trusted manner, user access to data based upon its classification.

4. **CAP Requirement.** Designated Approving Authorities (DAAs) shall ensure that all AISs under their jurisdiction are assessed for CAP compliance. DAAs shall document the system-specific information protection policy and corresponding CAP compliance features for each AIS, and include the documentation in the AIS accreditation records. The system may be of any scale (e.g., a base-wide

network) so long as the security policy and associated system access control components are clearly identified.

a. **Background.** The DON is experiencing an information technology revolution. Increasingly sophisticated computer technology is used within virtually every DON activity. As advances in automation continue, coping with increased risks to information and to systems is critical and must be addressed. Since these computer security risks are multi-faceted, reducing them to an acceptable level of risk requires solutions that effectively balance automated, procedural, physical, and personnel controls. CAP strengthens what has been historically the weakest link in the AIS security chain, protections against abuses by authorized users of the system.

b. **CAP Controls.** Automated controls provided by an AIS to ensure a fundamental level of protection:

(1) Control over who can log on to the system.

(2) Mechanisms that enable the AIS to make decisions regarding access to protected resources based upon the explicit permissions granted by the users or processes acting on their behalf. *These mechanisms are not highly resistant against concerted, malicious actions to bypass them.*

(3) The capability to generate a reliable log of user actions and to assure its correctness to the extent that a DAC policy is also adequately enforced; *e.g., executing an ill-behaved or malicious program will not be identified as a security breach, since it does not violate the DAC policy.*

(4) Mechanisms that enable the AIS to ensure that residual information left from one user's process will not be available to another user's process when the object containing that information is reused. See reference (d) for more specific guidance on object reuse. Note, Appendix A describes CAP features in detail.

c. **"Class C2" Criteria.**

(1) **Background.** DOD recognizes the general need for CAP features in AISs. DOD has established a "Class C2" (Controlled Access Protection) policy in reference (a). The DON implements this policy by reference (b). An underlying objective of this policy was to spur the development and commercial availability of products which provide the necessary controls to enforce DAC based information protection principles.

(2) **Criteria.** The "Class C2" criteria of reference (c), which is commonly known as the "Orange Book", prescribes a set of product design and evaluation criteria, or "classes", that meet hierarchically-ordered requirements for the security features and assurance characteristics needed to satisfy a range of control objectives. The Orange Book criteria are satisfied through **features** implemented in software, firmware, and/or hardware, and rigorous **assurances** achieved through managed design practices, documentation, and testing.

d. **Summary.**

(1) The fundamental CAP principles used in this guideline are based on "Class C2" criteria developed for *multi-user single computers* like mainframe and mini computers, reference (c). References (e) and (f) have adapted these for networks and databases. In each case, however, the focus is on the design, implementation, and evaluation of **products**, not application **systems**.

(2) Using a "Class C2" product by itself may provide the necessary foundation for achieving CAP. But it does not ensure that an entire associated system has all the required controls needed to enforce the specific information protection policies. Additional CAP controls may be needed in the application software, the network architecture, or in other protection domains.

(3) "Class C2" products can play a significant, but not necessarily complete, role in providing the security controls required to enforce the information protection policies and discretionary access control for an AIS.

*For example, consider a microcomputer-based LAN with a file server that uses an operating system with CAP features. The file server cannot provide CAP for data processed on the end-user microcomputers that are part of the LAN. It can only control the data while the data is centrally stored on the file server. If the file server contains database products which do not use the LAN operating system security features, then the file server operating system may not enforce applicable information protection policies over data handled by the database product. Instead, the database product may be entirely responsible for controlling access to database records, or fields, or whatever type of data object requires protection. Using a product with CAP features might contribute significantly towards the ability to enforce CAP on the microcomputer-based LAN but the operating system would be insufficient to enforce CAP by itself. Additional controls within the database product would be needed to enforce the applicable information protection policies.*

5. **CAP Waiver Criteria.**

a. **Authority.** Where there is a compelling cost or technical reason why a CAP feature cannot be implemented, it may be temporarily waived by the Waiver Approving Authorities (WAAs) authorized by the Secretary of the Navy (see Appendix B). *Waivers do not replace the responsibility to comply with CAP policy.* WAAs are responsible for formally granting a waiver, and for ensuring that local DAAs implement alternative mechanisms, develop plans for achieving compliance, and budget for resources required to procure automated controls. WAAs are also responsible for ensuring that local DAAs conduct a triennial review of all waivers until such time as full compliance with the CAP policy is achieved. Program Managers shall identify a single Development DAA (DDAA) for systems fielded into environments with multiple DAAs. The DDAA represents the remaining DAAs in certification decisions and will submit any required waivers to the cognizant WAA.

• **Stipulations for legacy architectures acquired prior to 31 December 1992.**

•• Most "single-user" architecture systems, like DOS-based and Macintosh personal computers, operate in the dedicated security mode and do not require CAP controls. However, when these "single-user" systems are operated in a "multi-user" manner requiring CAP controls, I&A, as a minimum,

shall be implemented. In addition, the WAA may require implementation of the other CAP features. Only I&A and the other features required by the WAA need a waiver.

- WAAs may delegate waiver authority only for "single-user" architecture, like DOS-based and Macintosh personal computers, as deemed appropriate.

- Program Managers shall include CAP compliance in the program review process and implement CAP in system upgrades as appropriate.

b. **Alternative Protection Requirements.** Where the CAP feature requirement is waived, a cost-effective approximation of CAP controls shall be used to enforce discretionary information protection and accountability policies. *One alternative strategy might be to use security products which provide controls in accordance with the set of criteria in reference (j) for computer security subsystems.*

c. **Limitations.** Even with a waiver, CAP safeguard requirements must be met. All AISs within the scope of this document must implement CAP. A waiver simply acknowledges that a sound basis exists to use features which do not fully comply with CAP, but which provide an appropriate level of security given the applicable cost-benefit considerations for the AIS.

d. **Triennial Waiver Review.** Until CAP features are implemented, WAAs will ensure a triennial review of any waivers granted under these guidelines. A triennial review is not required for those systems lacking only the object reuse portion of CAP controls. The permanent accreditation records shall include initial requests and all review documentation.

e. **Submission of Waiver Requests.** All requests shall be submitted to the appropriate WAA through the applicable chain of command. *Requests should be clear and concise and not exceed three pages in length.* The following are the minimum mandatory information elements for a waiver request:

(1) A summary description of the AIS, its system configuration, its major hardware and software components, and any CAP features employed.

(2) The information protection policy that applies, based on the sensitivity and value of the data processed. Sensitivity shall be determined in terms of confidentiality, integrity, and availability.

(3) A description of the nature and size of the authorized user community.

(4) An explanation of significant risks and any interim mitigating factors which have the effect of reducing the risk for the AIS.

(5) A concise cost-benefit analysis, either qualitative or quantitative, which justifies the waiver request.

(6) A requested waiver period which corresponds to the justification provided. *This may be "indefinite" for specific legacy architectures like DOS-based and Macintosh AIS CAP features.*

(7) A plan to comply with CAP policy that includes milestones and a time schedule. *This may not apply to legacy architectures previously mentioned.*

Security Mode	Architecture	Minimum required CAP features in:	
		initial waiver	triennial review
Dedicated	--	none	none
System High or MLS	Legacy "Single User"	I&A	I&A
	"Multi-User" or Non-Legacy "Single User"	TCB, I&A, DAC, AUD, and OR	TCB, I&A, DAC, and AUD

TABLE 1: Summary of Waiver Requirements

6. **CAP Assessment.** For a system to comply with CAP, the necessary features must be present in its products and those features must be functioning. Product assessments are useful in characterizing the CAP features prior to verifying their actual performance in an operational system. The operational verification should be performed during the Security Test and Evaluation phase of system accreditation.

a. **Types of Assessments.** The degree of analysis and/or testing required to verify CAP feature compliance will be based on the sensitivity of the information, the risks to its security, and the cost of alternative assessment approaches. Assessment alternatives can be generally divided into the following three categories, which are in order of the anticipated rigor of analysis and testing:

(1) **Basic Assessment.** Used to determine the **existence** of the set of CAP features within an AIS product. This can be determined through documentation reviews and analysis. A Basic Assessment does not encompass tests of specific features. A Basic Assessment is sufficient for AIS environments in which the information sensitivity to unauthorized disclosure or modification is low.

Reference (g) should be consulted for more specific guidance concerning Basic Assessments. *This type of assessment applies only to verifying that CAP features supposedly exist and are implemented in a manner that enforces the appropriate information protection policy. It does not imply any product evaluation.*

(2) **Detailed Assessment**. Used to determine whether the CAP features within an AIS product actually function as described or claimed. A Detailed Assessment verifies the positive conclusions of a Basic Assessment. It provides a higher level of confidence than a Basic Assessment because it tests specific controls. A Detailed Assessment is required for AIS environments in which information sensitivity to unauthorized disclosure or modification is high, but the AIS assessment risks appear to be relatively low. If it is cost-effective, a Detailed Assessment may also be done in conjunction with a Basic Assessment for AIS environments characterized by low information sensitivity. References (g) and (h) should be consulted for more specific guidance concerning Detailed Assessments. This type of assessment applies only to verifying that CAP features exist, function as described or claimed, and are implemented in a manner that enforces the appropriate information protection policy. It does not imply any product evaluation.

(3) **Recognized-Authority Assessment**. Similar in concept to the Detailed Assessment, but it also considers the product documentation and life cycle assurance in addition to verifying the CAP features of the AIS. Its verification also provides greater confidence that a product meets the CAP criteria because the assessment is conducted by or authorized and reviewed by organizations with established credibility in systems security analysis and testing. At the current time, DON recognizes the credibility of the following organizations with respect to CAP or "Class C2"-compliance assessments for AIS products:

- **NCSC** (National Computer Security Center)
- **NISE EAST** (Naval Command, Control and Ocean Surveillance  
Center ISE East Coast Division)
- **NRL** (Naval Research Laboratory)
- **AFIWC** (Air Force Information Warfare Center)
- **DISA/CISS** (Defense Information Systems Agency  
Center for Information Systems Security)

Reference (i) contains information on products which have received Recognized-Authority Assessments. When using them, consider any disparities that exist between the version of the product evaluated by the Recognized Authority and the version of the product being planned for use or currently implemented. If the versions are not the same, consider the risks associated with inferring conclusions about unassessed versions, based upon the results of assessments of subsequent or preceding product versions. *This assessment applies to verifying that the CAP product functions as described or claimed, and is implemented, with supporting assurances, in a manner that enforces a specific information protection policy.*

b. **Assessment Considerations.** While the CAP assessment approaches are identified in order of the degree of confidence they provide, this does not necessarily mean that the assessment costs (whether they be measured in dollars, operational impact, or otherwise) are always lowest for using a Basic Assessment and highest for a Recognized-Authority Assessment. For example, it would probably be more cost-effective for many mainframe systems to implement a Recognized-Authority assessed CAP featured or "Class C2" operating system or "add-on" security package combination (*e.g., MVS with RACF, ACF2 or TOP SECRET*) rather than attempt to conduct a Detailed Assessment using in-house resources. However, for other types of systems where the market for CAP-featured products is significantly less developed or the task of assessing is less complex, it may be more appropriate and/or more cost-effective to rely upon the Basic or Detailed Assessment alternatives.

c. **Security Mode Determination.** Each security mode determination must consider the AIS itself, its user communities, and the sensitivity of its data. When determining its mode of operation, user community, and sensitivity level(s), an AIS must be considered to be as large as its network. An AIS encompasses the full extent of electronic connection(s) among its component processors. Appendix C provides an example of a CAP security mode analysis.

*Example: A stand-alone microcomputer, not connected to any other processor through electronic communications, may be considered by itself when identifying the AIS's user communities and determining data sensitivity level(s). But if this same microcomputer were connected to a LAN, then the AIS would be the combination of the microcomputer and each of the other processors on the LAN. In this case, the users and the data sensitivity of the entire LAN, including each connected microcomputer, shall be considered to determine the mode in which the AIS operates (i.e., which security clearance and need-to-know attributes apply).*

(1) **Dedicated Security Mode AISs.** By definition, CAP controls are not *necessarily* required to be fully implemented for systems which operate in the dedicated mode. While such AISs do not necessarily require *automated* access and accountability controls, they still require protection.

*Example: Other protective measures are needed to distinguish non-registered persons, who are not authorized to access the system, from registered system users. Controls are required for restricting non-registered users from accessing data processed and stored by the AIS. Dedicated mode AISs may also require controls to ensure the integrity and availability of the information consistent with applicable information protection policies. Finally, they may require some types of accountability controls. While these controls are most often implemented using manual procedures, physical, and personnel controls, they can often be efficiently implemented by automated features.*

(2) **System High Security Mode AISs.** These AISs are the target of CAP controls. CAP provides the necessary need-to-know and need-to-modify protections for the information contained within the AIS.

(3) **Multilevel Security Mode AISs.** For multilevel AISs CAP controls represent only a subset of the required controls. CAP is **inadequate** to protect classified information from access by insufficiently cleared system users for two reasons. First, CAP systems do not include appropriate security **features** for enforcing mandatory information protection policies. Discretionary information

protection policies do **not** allow for security administrator domination in authorizing access. Second, CAP systems are **not** designed with a sufficient level of **assurance** to compensate for risks associated with having classified information and inadequately cleared users on the same system. Thus, **this document does not address the specific security features and the level of assurance required for AISs operating in the multilevel mode**

d. **Inherent AIS Assessment Risk**. The AIS assessment attempts to describe the characteristics of the CAP features. The risks in correctly performing this characterization are tied to the CAP compliance assurance. The following are examples of factors to consider when evaluating inherent AIS assessment risks. It is not necessarily an all-inclusive list.

- Complexity of the product to be assessed.
- Nature and size of the authorized user community which accesses the AIS where the product will reside.
- Complexity and extent of the AIS configuration in which the product will reside.
- Configuration differences from previously evaluated products.
- Nature and extent of the product's interaction with other software and/or hardware of the AIS in which it will reside.
- Extent to which the product will be relied upon to enforce the applicable policies mandated to protect information (*e.g., classification guides, Privacy Act of 1974*)

Consider the inherent AIS assessment risks associated with evaluating a general purpose operating system for mainframe or minicomputer systems. Such risk would almost always be considered high because such operating systems are typically very complex and often must be relied upon to enforce significant aspects of information security policies relevant to resident data and programs. It should be noted that almost all products or development efforts which *claim* "Class C2" compliance are likely to involve relatively complex technology and will often be used in areas involving high risk.

e. **Assessment Selection Guide**. The following table summarizes the acceptable approaches for assessing compliance with the CAP requirement, depending upon data sensitivity and AIS control risks. Where there is a choice of approaches, the most cost effective approach shall be used. Since the costs of the respective assessment approaches cannot necessarily be inferred from Table 2 select the proper assessment approach on a case-specific basis.

		INHERENT AIS ASSESSMENT RISKS	
		LOW	HIGH
INFORMATION SENSITIVITY	L O W	<b>Basic or Detailed or Recognized- Authority</b>	<b>Basic or Detailed or Recognized- Authority</b>
	H I G H	<b>Detailed or Recognized- Authority</b>	<b>Recognized- Authority</b>

*TABLE 2: Assessment Selection Matrix*

## APPENDIX A

### TECHNICAL CONSIDERATIONS FOR CONTROLLED ACCESS PROTECTION (CAP) FEATURE IMPLEMENTATION

- Ref:
- (a) DOD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria
  - (b) NCSC-TG-017, A Guide to Understanding Identification and Authentication in Trusted Systems
  - (c) NCSC-TG-003, A Guide to Understanding Discretionary Access Control in Trusted Systems
  - (d) NCSC-TG-018, A Guide to Understanding Object Reuse in Trusted Systems
  - (e) NAVSO P-5239-26, Department of the Navy Information Systems Security Guidelines, Remanence Security Guidebook
  - (f) NCSC-TG-001, A Guide to Understanding Audit in Trusted Systems

1. **CAP.** CAP contains a fundamental set of security functions regardless of design, implementation, or platform selection. The Trusted Computing Base (TCB) is the architectural foundation for these security functions. They include: Identification and Authentication, Discretionary Access Control, Object Reuse, and Audit. Since these functions are interrelated in ways where deficiencies in one area can adversely affect the others, both individual and combined performance shall be considered.

2. **Definitions.** The CAP feature descriptions in this enclosure are for education and illustration purposes. If exact semantics are required, reference (a) should be consulted. The two terms below are fundamental for understanding DOD trusted computer systems and CAP.

a. **Object.** Any passive entity that contains or receives information (*e.g., files, directories, records, blocks, pages, segments, programs, video displays, printers*). Access to an object implies access to the information it contains.

b. **Subject.** Any active entity in the system (*e.g., person, process (i.e., an executing program), or device*) that causes information to flow among objects or changes the system state (*e.g., from operating on behalf of the system to operating on behalf of the user*)

3. **Trusted Computing Base.** Controlled access protection features are contained in a Trusted Computing Base (TCB) (*for purposes of this discussion, those modules of code containing the security function*). The TCB enforces a security policy which, with some degree of assurance, makes sure the CAP features cannot be readily circumvented by higher level system features (application programs) or users. For any AIS, the TCB includes all software, firmware, and hardware components responsible for enforcing the security policy as well as components that may affect the correct operation of the security mechanisms. Thus, the TCB includes components that perform security functions required to enforce the security policy (*e.g., programs that check file access control settings*) and components that have no direct functionality relative to the security policy, but require privilege(s) to operate and therefore shall be trusted (*e.g., a device driver dealing directly with the underlying hardware*).

a. **TCB Elements.** As the basis of CAP, a "Class C2" TCB supporting CAP is typically large, dispersed, and generally unstructured. Although its elements are difficult to analyze, the TCB shall have these characteristics:

(1) The TCB shall maintain a domain (sometimes called a privileged address space) for its own execution that protects it from external interference or tampering.

(2) Protected resources controlled by the TCB may be a subset of subjects and objects in the system.

(3) The TCB shall isolate protected resources so that they are subject to access control and auditing.

b. **TCB Element Scope**. The scope for a TCB depends on the AIS being protected (network or single system) and the granularity of its protected entities (files, memory areas, or database fields). While in limited cases (*e.g., where a database manager is the **only** user application interface*) the protection critical components of the TCB can reside solely in the application, normally, the TCB begins at the operating system (including the network level) and encompasses those trusted applications necessary to support the AIS's security policy. Thus, typical multi-user operating systems shall maintain privileged states (instruction and/or address capabilities) separate from those available to user programs.

4. **Identification and Authentication (I&A)**. CAP mechanisms ultimately depend upon the trustworthiness inherent in the AIS's I&A mechanisms. Unless trust can be placed in the system's ability to accurately, consistently, and positively identify each user, and to maintain that positive identification throughout the user's log-on session, controlled access protection cannot be assured. Moreover, any audit data collected cannot be reliably used for personal accountability. For this reason, if the system lacks acceptable I&A mechanisms, it cannot be CAP compliant. Reference (b) discusses the I&A requirement at length and provides guidance on how to design and implement effective I&A mechanisms.

a. **I&A Objectives**. CAP seeks to control users' access to information in the AIS; specifically, information contained in objects to which users can refer by name (*e.g., files*). All forms of access control rely on the system's ability to identify users and to prove their identity when they log on to the system, and to maintain a positive association between each individual user and the actions for which he or she is responsible.

b. **I&A Mechanisms**. Identification is generally implemented by simply asking for a log-on name, usually associated in some way with the person's identity. This name is checked against the system's authorized users. Then, to protect against an unauthorized user's masquerading as the authorized user, the system asks for some "proof" (authentication) that the user is whom he or she claims to be. One or more of three types of "proof" is generally used for authentication: (1) something the user knows (*e.g., a password*); (2) something the user has (*e.g., an authentication device*) or, (3) something the user is (*e.g., a retinal scan*)

c. **I&A Integrity Considerations**. Most AISs implement I&A using the simple, but acceptable, log-on name and password technique. Other AISs strengthen their password mechanisms by enforcing rules such as aging and length requirements, or by providing random-password generators. However, as with any mechanism, the integrity of the password protection is only as strong as the integrity and responsibility of the users. In any event, passwords should be difficult to guess, protected (including during their passage through a network), and changed regularly.

5. **Discretionary Access Control (DAC)**. Controlled Access Protection enforces a security policy principle known as "Discretionary Access Control." DAC features restrict access to named objects based upon the identity of subjects and/or groups to which they belong. In systems that have DAC features, a data "owner" can protect and control objects by specifying which users or user groups may have access to them.

a. **DAC Mechanism Types** Five mechanisms have been used to implement DAC:

(1) **Access Control Lists**, which implement a matrix, where the columns represent users, the rows represent protected objects, and each cell indicates the type of access granted for the associated subject-object pair.

(2) **Protection Bits**, which use a bit vector, where each bit represents a type of access. The most common example is the Unix nine-bit vector reflecting read, write, and execute access to be granted to the object's owner, a group, and everyone else.

(3) **Capabilities**, in which access to a protected object is granted if the requester possesses the appropriate "capability" that both identifies the object and specifies the access rights to be allowed to the user who possesses that capability.

(4) **Profiles**, which associate each user with a list of protected objects that the user may access.

(5) **Passwords**, which associate one password for all types of access or multiple passwords for different types of access.

b. **DAC Precautions**. These mechanisms are described in greater depth in reference (c). DAC provides individual users and groups the ability to specify whether other users and groups on the AIS should be given access to their objects (*e.g., files and directories*) and, if so, the kinds of access they should be given. However, while most DAC implementations can adequately protect objects in many circumstances, they do not defend against ill-behaved or malicious programs on the system. This occurs because as such programs run, they often assume the privileges associated with the user who invoked them. Subsequently, these programs may be able to transfer privileges to a third-party who would otherwise be forbidden to have them. Therefore, DAC-enforced access rules are insufficient for protecting objects with different classification levels or categories (strict or formal need-to-know separation).

6. **Object Reuse**. To meet the object reuse requirement, the AIS shall ensure that residual information left by one user's process will not be available to another user's process when the object containing that information is reused. The objective is to prevent information from being inadvertently (and by extension, deliberately) disclosed to unauthorized users. In contrast with the DAC mechanism, which seeks to protect the information containers themselves (*i.e., named objects*), the object reuse requirement seeks to protect the information contained in those objects. Several approaches for meeting the object reuse requirement exist and are specific to the object containers being considered. Whether the object reuse mechanisms operate "before" use or "after" use is a designer's choice -- either method is acceptable. References (d) and (e) provide detailed information about object reuse mechanisms.

7. **Audit**. Audit features support DOD policy requirements for assigning personal accountability for actions taken while accessing or using an AIS, its features, and/or information. While auditing can determine what went *wrong*, it is equally valuable for determining what went *right*. Importantly, audit policy requires that the AIS be **capable of** auditing, but not that it actually **performs** auditing. Determining which auditable events to select for the system is a DAA responsibility. The Information Systems Security Officer (ISSO) responsible for the AIS activates the specific mechanisms or functions accordingly.

a. **Audit Mechanisms**. Audit is the capability to record, examine, and review security-relevant activities for an AIS either as they occur or retrospectively. Real-time auditing capabilities are not required in order to meet CAP objectives. Rather, the AIS shall audit features that can be configured to record the set of

events specified by the DAA, to present this information in a useful manner when needed, and to monitor users' actions in order to anticipate and potentially neutralize impending security attacks. Reference (f) discusses five objectives of an audit mechanism:

- (1) For reviewing access patterns for individual objects, access histories for specific processes and users, and the use (or abuse) of various protection mechanisms and their effectiveness.
- (2) For detecting repeated attempts to bypass protection mechanisms.
- (3) For monitoring use of privileged functions or capabilities.
- (4) For deterring habitual attempts to bypass the system protection mechanisms (*i.e., users know that their actions can and may be audited*)
- (5) To provide additional assurance that the protection mechanisms are working as specified.

b. **Audit Integrity Considerations**. As stated earlier, audit mechanism integrity depends on I&A mechanism integrity. That is, unless users can be positively identified, actions cannot be correctly associated with them. As with all CAP mechanisms, audit features shall be implemented by the TCB. Moreover, only the ISSO should be able to invoke or curtail auditing as well as to configure the audit mechanism itself (*e.g., events to be recorded*). Furthermore, audit trail data shall be strictly protected by the TCB against unauthorized modification or loss (*e.g., a circular file recording technique might overflow*); only designated persons should be able to read audit trail data.

c. **Audit Trail Events** The AIS shall be able to record the following types of events:

- Use of identification and authentication mechanism(*i.e., log-on*).
- Introduction of objects into a user's address space (*e.g., file open, file creation, program execution, file rename*)
- Deletion of objects from a user's address space (*e.g., file close, completion of program execution, file deletion*)
- Actions taken by computer operators and system administrator(*e.g., adding a user*)
- All security-relevant events(*e.g., use of privileges, changes to DAC parameters*)
- Producing printed output.

d. **Audit Trail Event Records**. For each auditable event, the following information shall be recorded:

- Date and time of the event.
- Unique identifier of the user on whose behalf the program generating the event was operating.
- Type of event (one of the above).
- Success or failure of the event(*e.g. failed login, execution of program*)
- Origin of the request (*e.g., terminal identifier*)for identification and authentication events.

- Name of the object that was introduced into or deleted from the user's address space.
- Description of modifications that the system administrator makes to the security databases.

e. **Audit Trail Tools**. The ISSO shall be able to audit on individual or object identity. Whether the system allows the ISSO to pre-specify individuals and/or objects, or a post-processor is available to extract data associated with specified individuals and/or objects, is an implementation decision. Either approach is acceptable.

f. **Audit Precautions**. Based upon operational requirements the DAA may select a subset of the items and their attributes (*e.g., granularity -- data set volume versus data set file*) described above for implementation as audit capabilities in an AIS. While this is acceptable under DON CAP guidance, the DAA should understand that these reductions will be a deviation from historically effective auditing capabilities.



**APPENDIX B**

**CONTROLLED ACCESS PROTECTION (CAP)  
WAIVER APPROVING AUTHORITIES (WAAs)**

Assistant for Administration, Office of the Under Secretary of the Navy  
Chief, Bureau of Medicine and Surgery  
Chief, Bureau of Naval Personnel  
Chief of Naval Education and Training  
Chief of Naval Operations (N643, N514)  
Chief of Naval Research  
Commandant of the Marine Corps (C4I)  
Commander-in-Chief, Atlantic Fleet  
Commander-in-Chief, Pacific Fleet  
Commander-in-Chief, U.S. Naval Forces, Europe  
Commander, Marine Corps Air Bases, Eastern Area  
Commander, Marine Corps Air Bases, Western Area  
Commander, Marine Corps Bases, Atlantic  
Commander, Marine Corps Bases, Pacific  
Commander, Marine Corps Logistics Bases, Albany, GA  
Commander, Marine Corps Systems Command  
Commander, Naval Air Systems Command  
Commander, Naval Computer and Telecommunications Command  
Commander, Naval District Washington  
Commander, Naval Facilities Engineering Command  
Commander, Naval Information Systems Management Center  
Commander, Naval Investigative Service Command  
Commander, Naval Legal Services Command  
Commander, Naval Oceanographic Command  
Commander, Naval Reserve Force  
Commander, Naval Sea Systems Command  
Commander, Naval Supply Systems Command  
Commander, Space and Naval Warfare Systems Command  
Commanding General, Fleet Marine Force, Atlantic  
Commanding General, Fleet Marine Force, Pacific  
Commanding General, Marine Reserve Forces, New Orleans, LA  
Commanding General, Marine Corps Combat Development Command  
Commanding General Marine Corps Recruit Depot, Eastern Recruiting Region,  
Paris Island, SC  
Commanding General, Marine Corps Recruit Depot, Western Recruiting  
Region, San Diego, CA  
Director, Strategic Systems Programs  
Office of the Navy Comptroller

THIS PAGE INTENTIONALLY BLANK

## APPENDIX C

### EXAMPLE CAP SECURITY MODE ANALYSIS

**Scenario.** This example is the administration and management system, named DOALL, on the USS Neversail. DOALL is composed of stand-alone PCs, networked PCs, file and print servers, and multi-user Unix systems. While there are other PCs and servers in DOALL, those described here are representative of the system. The PCs have hard disks and execute Microsoft DOS and Windows™. The PC-server architecture is client-server so that only the user of the PC can invoke applications to access user data on the PC. (Peer-to-peer architectures can also be configured with similar restrictions for user workstations.) The PCs act as intelligent terminals when connected to a Unix system. The network is physically protected against access from unauthorized users.

a. Server1 and Server2 are located in the admin section and are administered by DP1 Coder and DP2 Count. These servers contain application programs (e.g., Microsoft Word™, Lotus 1-2-3™, cc:mail™, etc.); personnel, logistics, and financial databases; and, corresponding word processing text files. Server1 supports two printers. Server2 supports the activity's e-mail. All users have unique login IDs. All officers and chiefs have private disk directories on Server2. There is no private storage allocated for other users.

b. CRACKLE is a standard Unix-based system which executes an application program providing personnel, logistics, medical and financial databases. The Program Manager, COMSPAWARSYSCOM, is responsible for the certification of the system and coordinating with the Development DAA, CINCLANTFLT, for the submission of any necessary CAP waiver request. CRACKLE is administered by DP1 Coder. Users are restricted to executing the database program and cannot access the core Unix functions. PC1 through PC3 use X-Window protocol to connect to CRACKLE.

c. PC1 is located in LCDR Anchor's office and she is the sole user. She connects to the servers to update and review ship logistics records and to access a printer. She stores copies of personnel actions for her section on the system's nonremovable disk.

d. PC2 and PC3 are located in the maintenance section and are used by all the section personnel. Local printers are attached to each system. Both PCs connect to and use a logistics database stored on the servers. PC2 has a terminal emulation program and a built-in modem which are used to connect to a parts ordering system located at a shore activity. CPO Wrench uses PC3 to prepare personnel evaluations which he stores on a floppy diskette which he normally keeps in a locked cabinet.

e. PC4 is a stand-alone system located in operations and is used by the section chiefs. It has two removable hard disk drives and is used to prepare and distribute message diskettes.

f. PC5 is a stand-alone system located in a passageway. It executes a locally developed application which allows individuals to submit and review responses from their detailers. This personnel data is covered under the Privacy Act of 1974. In its present version users can view or modify any entry in the system.

**Analysis.** This analysis uses the information provided in the developer's literature and constitutes a basic assessment. Since all the users of DOALL are authorized access but do not have need-to-know or need-to-modify for all of the data in the system, the system operates in the system-high security mode and requires CAP controls.

a. Server1 and Server2.

(1) TCB. Satisfied. Only the server software executes on the TCB; there is no user software which is executed. The only subject is the user connection to the server. Vendor software updates which correct all known security vulnerabilities have been installed.

(2) I&A. Satisfied. All users have unique login IDs and passwords are used.

(3) DAC. Satisfied. Objects which are protected are files and printer queues. Directories have access control lists configurable at the user and group ID level for the properties of read, write, and execute. Database programs control access to the field level using their own internal mechanisms. Printer queues can be altered by the owner of the print object and the administrator. The administrator has access to all server objects.

(4) AUD. Satisfied. User logins, login attempts, and attempts to access protected directories are audited. While this does not encompass all audit events identified in CAP it is sufficient to support the subset required by the local security policy.

(5) OR. Satisfied. Users cannot access storage objects containing data released by other users during normal system operation. The administrator can access these storage objects when the server is configured in maintenance mode. Since the administrator has access to all file and storage objects anyway, this is not a violation of the DAC policy.

b. CRACKLE.

(1) TCB. Satisfied. Only the CRACKLE software executes on the system; there is no user software which is executed. Vendor software updates which correct all known security vulnerabilities have been installed.

(2) I&A. Satisfied. All users have unique login IDs and passwords are used. Users are identified at both the operating system and the application level.

(3) DAC. Satisfied. Users access objects at the field level within the database applications. Protections are provided by the operating system under separate database files and by the database applications themselves. The pairing of control also exists for access to peripherals. General users cannot directly access the Unix operating environment. This access is reserved for system administrators.

(4) AUD. Satisfied. A robust set of auditing capabilities exists. The minimum default set has been reviewed by the DAA and satisfies the security policy.

(5) OR. Satisfied. Users cannot access storage objects containing data released by other users during normal system operation. The administrator can access these storage objects when the system is configured in maintenance mode; this is not a full implementation of object reuse. But, since the administrator has access to all file and storage objects anyway, this is not a violation of the DAC policy.

c. PC1 operates in the dedicated mode. PC1 has only one user and access is controlled by practices and procedures.

d. PC2 and PC3 operate in the dedicated mode; all of the data is common and shared. Practices and procedures ensure that only authorized users can access these PCs. Although CPO Wrench stores his personnel data to floppy disks certain characteristics of the DOS single-user operating system may cause copies of the data to be retained on the hard disk where it is not protected under object reuse. Similarly, PC2 and PC3 may retain user IDs and passwords associated with connecting to the servers. This security deficiency can be overcome by releasing and overwriting the offending objects after each user finishes their session on the PC. But, unless required by the WAA, this deficiency has been deemed an acceptable risk under CAP and no corrective action is required.

e. PC4 also operates in the dedicated mode. Practices and procedures ensure that only authorized users can access this PC.

f. PC5 does not provide adequate need-to-know and need-to-modify protection for the personnel data. This system should be operating in the system high security mode, but it offers only dedicated mode protections. Since PC5 was acquired in December of 1992, CAP requires that at least Identification and Authentication be applied to PC5 to ensure access is limited to authorized users.

**Summary:** With the exception of the stand-alone system PC5, DOALL and its component systems are CAP compliant. If this PC cannot be configured to support I&A, a waiver request must be submitted for this component of DOALL.