CA-Top Secret®

Planning Guide
Release 3.0
VSE

SP1

Second Edition, September 2000

Contents

About This Guide

Purpose

This guide provides guidelines to aid you in planning the effective implementation of CA-Top Secret Security. It presents all of the considerations for planning your security implementation in one convenient document. This enables you to review the entire security implementation project before you begin to plan for your own organization. Recommendations are presented, along with tradeoffs which you should consider when selecting among recommended options.

The recommendations are not merely textbook suggestions, but rather the result of observing what happens when the security implementation is **not** properly planned. Security implementation problems experienced by CA-Top Secret customers who report them to the CA-Top Secret support staff are often a direct result of inadequate planning given to one or more of the critical steps discussed in this guide.

Intended Audience

This information is intended for:

- security administrators and other personnel responsible for enforcing security,
- systems and operations personnel responsible for the implementation of security,
- auditors, and
- management and other staff involved in the implementation of security.

Prerequisites

It is assumed that you have a basic knowledge of data processing and security concepts and that you have read the CA-Top Secret *User Guide.* The *Planning Guide* compliments the *User Guide.* As such, you may refer to the *User Guide* as you read the *Planning Guide* material.

Organization

Chapter	Description
1	Describes the objectives of the Planning Guide.
2	Outlines the elements of a well-written security policy or statement of direction.
3	Provides guidelines to determine where security information resides and who handles security functions.
4	Describes how to assign a security implementation team.
5	Provides guidelines to plan and schedule the security implementation plan.
6	Lists basic product knowledge prerequisites and the sources for additional product information.
7	Identifies the password controls and standards.
8	Lists control options you must review before product installation.
9	Reviews the backup and recovery procedures.
10	Describes the resource/user inventory and exposure analysis.
11	Introduces guidelines for establishing and using resource naming standards.
12	Provides guidelines for designing security file structure.
13	Describes the way to refine the security administration structure.
14	Defines procedures for handling violations.
15	Lists security maintenance procedures.
16	Reviews testing procedures.
17	Describes situations that may require product customization.
18	Discusses converting from other security software to CA-Top Secret.
19	Addresses the goals and procedures for a successful security awareness program.
20	Describes how to schedule ongoing product evaluation.
Appendix A	Contains Corporate Level and Application Level Policy examples.
Appendix B	Shows a sample inventory form.
Appendix C	Shows a sample maintenance form.
Appendix D	Contains a sample user guide.
Index	Provides an efficient way to locate specific material.

CA-Top Secret Publications

The following publications are supplied with CA-Top Secret:

Title	Contents
Installation Guide	CA-Top Secret installation for VSE, including: installation and maintenance steps, startup and shutdown considerations, backup and recovery procedures, and Security File conversion.
Command Functions Guide	Comprehensive reference to the TSS command and CA-Top Secret resources.
Control Options Guide	Comprehensive reference of CA-Top Secret control options.
Implementation: BATCH, STC and APPC Guide	Provides for setting up security in Batch, STC and APPC environments.
Implementation: CICS Guide	Provides for setting up security in a CICS environment.
Messages and Codes Guide	Provides all CA-Top Secret messages and codes.
Planning Guide	General guide for planning a successful CA-Top Secret security implementation and describing the latest enhancements to CA-Top Secret.
Report and Tracking Guide	Details the use of TSSUTIL, TSSTRACK, TSSAUDIT, TSSCFILE and TSSCPR and provides sample reports.
Troubleshooting Guide	Includes CA-Top Secret debugging options and facilities, information to be prepared prior to contacting Technical Support, and an explanation of customer support.
User Guide	Conceptual overview of CA-Top Secret architecture and capablilities. Also includes implementation instructions that span all facilities, including: implementation how to's, customization, and the CA-Top Secret utilities.

All guides are updated as required. Instructions accompany each update package.

Related Publications

The common component services formerly known as CA90s have been enhanced and renamed CA Common Infrastructure Services, CA-CIS. All the documentation for the services exists in the following publications supplied by Computer Associates:

Name	Contents
CA-CIS Administrator Guide	A guide for system administrators.
CA-CIS CAICCI User Guide	Describes how to use the communication protocols needed for cross-system communication.
CA-CIS Installation Guide	Tells how to install the CA-CIS.
CA-CIS Message Guide	Lists messages and codes for CA-CIS.
CA-CIS Reference Guide	Describes how to access and use the VSE common components.
CA-CIS Systems Programmer Guide	Details the programming requirements for command, security, and signon exits.

The following publications relate to CA-Top Secret and are available from Computer Associates:

Title	Operating System
CA-EARL Reference Guide	MVS/VM/VSE
CA-EARL User Guide	MVS/VM/VSE
CA-EARL Systems Programmer Guide	VSE
CA-EARL Examples Guide	MVS/VM/VSE

Command Notation

Enter the following exactly as they appear in command descriptions:

UPPERCASE	identifies commands, keywords, and keyword values which must be coded exactly as shown.
MIXEDcase	identifies acceptable command abbreviations. The UPPER-CASE letters represent the minimum abbreviation possible. The lowercase letters of the command may be entered for further clarification **Note:** In some cases, the command processor may require a more detailed abbreviation due to user-defined resource being the same as a command abbreviation. In these cases, either enter the complete command or code a national or numeric character in one of the first four positions of the user-defined resource.
underlining	identifies default operands. These operands do not need to be entered to take effect.
Symbols	"" / * # () , must be coded exactly as shown.

The following items clarify command syntax; do not type when they appear:

lowercase	indicates keyword values which you must supply.
[ ]	identifies optional keywords.
|	separates alternative keywords or values; choose one.
{ }	indicates that you must enter one of the keywords.
...	means the preceding value may be repeated more than once.

The following table indicates the appropriate command format.

Sample Command	Explanation
TSS PER(acid) DSN(dsname)	You must supply a value for the ACID and for the data set name.
MODE(DORM|IMPL|WARN|FAIL)	You must choose **only** one of the keywords.
TSS {ADDto } (acid) MCSAUTH {(INFO) } {REMove } {(MASTER)} {REPlace} {(SYS) } {(IO) } {(CONS) } {(ALL) }	You must select a command function, enter the name of an ACID, enter the MCSAUTH keyword, and select an operand from the list.

Chapter 1. Introduction

Prior to beginning the security implementation process, it is crucial to create a workable implementation plan. The main objective of this document is to show you how to design an effective plan and guide you in making the correct decisions during the development and implementation of security.

1.1 Objectives

After reading this guide, you should be able to:

- Identify and formulate a direction for security.
- Establish job functions and assign to areas responsibilities for the various tasks required to implement security.
- Develop implementation plans and assign implementation teams.

As with attempting to meet any objectives, a set of conditions need to be understood. Your installation's CA-Top Secret implementation plan should be based on the following premises:

- CA-Top Secret Is a Means to an End

  Your environment is not secure immediately after installing CA-Top Secret. CA-Top Secret is the tool used to build a secure data processing installation. Therefore, each installation must plan and design their security implementation to conform to the needs of their environment. Much work is involved in implementing any security package, and this work is not entirely technical, as you will learn in the following chapters.

- Implementation Requires Adequate Support

  A security implementation does not go quickly, and it requires much internal support. If security is an important concern in your environment, then it must have the proper support in terms of management direction, manpower, and resources. It is best to take the time to evaluate the environment and carefully plan the implementation. A rushed implementation, just as any other rushed project, often requires rework and redesign down the road.

- Security Is a Global Concern

  The corporate area assigned to handle security administration is not the only area that needs to be concerned with security and the security product. Security is not a function that can be restricted to one area. It is an environment consisting of every person involved in the data processing function—from the EDP auditors to the end-users. Without the support of all individuals, it is unlikely that security will ever be taken seriously within your organization.

- Security Implementation Is Ongoing

  The security implementation never ends. After total implementation of CA-Top Secret, you will find that your use of CA-Top Secret must be continually adjusted to reflect changes which occur within your installation. Your CA-Top Secret implementation is just as dynamic as your data processing environment. It will require continual analysis, review, and modification to properly protect your installation.

1.2 The Remaining Chapters

The following chapters detail the steps required to successfully implement CA-Top Secret. Although it is not necessary to follow these steps in order, it is recommended that each step be detailed somewhere in your implementation plan, and that you allot the appropriate time allowance for completion. You may find that some steps can be addressed concurrently in your installation while others must be single-threaded. You can choose the most appropriate order for your installation after you have reviewed the material in this guide.

Chapter 2. Formulating a Security Policy

This chapter outlines the elements contained in a well-written security policy or statement of direction. A major element of a security policy is the statement of what area of the data processing installation will be responsible for each aspect of security administration. This element is examined in detail in this chapter.

2.1 Statement of Goals

As in any major project, you must detail your security implementation goals before you set out to achieve them. Policy, or minimally a document of security objectives, should be developed before the implementation is begun. This is another excellent reason for drafting a security policy, which goes beyond objective-driven project management.

2.1.1 Gain Support for Security Implementation

Management support is critical during the implementation of security. Even more important than your selection of CA-Top Secret as your security implementation tool, is the proper creation of an attitude throughout your organization that emphatically supports the implementation of security. To successfully implement CA-Top Secret, this attitude must be encouraged at the highest level. No security software will stop cooperative parties in strategic positions from violating the security software and procedures. Policies must be established that indicate the importance and level of security required for the particular environment. These policies must be communicated to all individuals who use the data processing facilities as part of their job function.

2.1.2 Scope of Security Policy

The security policy might confine itself to addressing only those issues relating directly to security software, or it can be a part of a more global security policy which addresses issues including physical security, employee identification, employee clearance, and privacy of personal information. The following discussion addresses only the security software implementation issues.

2.2 Primary Elements of a Security Policy

Minimally, the security policy or document of security objectives should address the following areas:

1. Objectives or premises that prove the need for security in your environment.
2. Scope of security. What is to be protected (for example, data, data processing facilities, hardware).
3. Ownership of resources. Who owns the data processing resources (such as data, facilities, and hardware).
4. Responsibility for the integrity of the resources. Who is responsible to ensure that resources are being accessed, used, or modified in a secure manner.
5. Requirements to access the resources. Who needs access. Requirements may also specify those job functions authorized to determine when an individual requires access to a resource.
6. Statement of intent as to how violations are to be logged and reported.
7. Accountability. Action to be taken when security is breached.
8. Account protection requirements. In password-based security systems, this protection could include change intervals, one account per employee, and account assignment for remote users. This approach assumes that:
    a. Access to data processing facilities and data is company property granted to the employee to perform a specific job function.
    b. Each employee is responsible for the use of his account.
9. Responsibility for the support and enforcement of the direction statement by functional area, including that of the security administration area.

Many policies elaborate on this last point, since it states specifically what is expected of each functional area in the support and enforcement of the policy. Each user of the data processing facility must understand that he has a role to play in the security scheme and must understand what that role is.

2.3 Functional Areas and Their Responsibilities

The following sections discuss the typical functional areas in a normal environment and what their responsibilities should include.

2.3.1 Security Administration

Centralized: The central security administration area should be the focal point of the security effort, with a minimum objective of giving all users an ultimate point of reference in security matters.

Consider the following responsibilities for this area:

1. To develop the standard security procedures to be used within the corporate environment.
2. To document the security controls available and communicate them to all appropriate security system users.
3. To estimate the risks and exposures within the corporate environment.
4. To administer security within the guidelines of the policy.
5. To log and report violations to the appropriate individuals.
6. To assist in the development of security designs for all user requirements.
7. To educate all users in corporate security policy and in the use and features of the security software.
8. To support and monitor decentralized administration where decentralization is required.

Decentralized: A statement on the appropriateness of decentralized security administration should be detailed in the policy. If decentralization is included as a viable means of administration for the environment, responsibilities of each area should be detailed.

Here are some of the typical responsibilities of a decentralized security administrator:

1. To assist the central security administrator within the guidelines of the policy.
2. To handle security administration requirements for the areas which fall within her scope.
3. To assist in the development of security designs for all user requirements which fall within her scope.
4. To report violations to the appropriate authorities and provide follow up activity on same.
5. To document security controls that exist within her scope.

2.3.2 Systems Software Area

The systems software area is an area that must be considered critical in any organization. The security software is the responsibility of this area. The systems software personnel often use facilities that are capable of bypassing or even disabling the security software.

The policy must detail the responsibilities of this critical area as it relates to security. Consider identifying the following responsibilities for systems software:

1. To maintain the security software in a secure and responsible manner, ensuring that the data processing environment is always protected when it is available for use by the user community.
2. To notify the appropriate parties, as soon as is practical, if the security software is disabled.
3. To limit development and availability of facilities capable of bypassing security to only those situations in which they are absolutely necessary.
4. To work with the security administration function to ensure that system resources are properly protected.
5. To design the security requirements for the vendor-supplied system software for which they are responsible, and to work with the security administration area in implementing those requirements.

2.3.3 Applications Software Areas

The applications areas must interface properly with the security areas to ensure that application resources are properly protected. Each application area will be the best source of information concerning how best to protect an application, since each application will differ to some extent.

Consider the following responsibilities:

1. To define the security requirements for the application, and to work with the security administration area in implementing security for the application.
2. To notify the appropriate security administrator of all revisions to the application that will affect the security design.

2.3.4 The Auditing Function

The auditors should be responsible for monitoring the effectiveness of the security procedures and controls. Consider assigning the following responsibilities to them:

1. To monitor all responsible areas to ensure that they adhere to the security policy.
2. To audit the use of all critical system and application resources.
3. To periodically monitor user activity.
4. To monitor the access requirements set by the security administration area.

2.3.5 Operations

The operations area is responsible for scheduling, controlling, running, and distributing the production processing. Because of the powerful requirements of this area, consider assigning the following responsibilities to them:

1. To handle all responsibilities of production processing in a secure manner.
2. To access all resources only through the production facilities developed by the systems and applications software areas, and only for the purposes defined by those facilities.

2.3.6 All Users

General responsibilities can be assigned to all users regardless of functional area. This principle is based on the premise that it should be the obligation of all users to protect the corporate data processing assets. Consider assigning the following responsibilities to the general user community:

1. To keep confidential all accounts used to access data processing resources and facilities.
2. To revise the password to these accounts at regular intervals.
3. To notify the appropriate areas if abuse of an account is suspected.
4. To actively support all security procedures.

2.4 Ensuring User Accountability

Many organizations add the responsibility for adherence to and support of security measures to job descriptions. Some organizations take this a step further and ask each employee to sign a compliance agreement whereby they agree to follow the security policies and procedures in effect for the organization.

Compliance is monitored as part of the regular job and/or performance review. This can be an effective additional method for gaining active support of security policy and procedures by every employee. If employees are aware that their performance will be evaluated, in part, by their adherence to security policy, then it will be generally understood that your organization takes security seriously.

2.5 Levels of Security

There are two levels of security policy that can be considered:

- the corporate level
- the application level

Corporate Level: A corporate level of globally acceptable security measures and procedures is the typical level of policy that is issued for general distribution to all users of the data processing facilities. This is the type of policy being discussed.

Application Level: There are often applications that require additional measures above and beyond the level set by the corporate policy. Specific policies can be developed which detail the additional security requirements necessary for facilities such as: accounts payable, human resources, or particularly sensitive facilities. These policies may be distributed to only the necessary functional areas.

2.6 Conclusion

There are samples of corporate level and application level policies in Appendix A. These policies were submitted by CA-Top Secret customers as a suggested base for your own security policies.

No matter what form your policy takes, the critical point in the security implementation is that direction be set and communicated before the implementation begins. Without this direction, the security implementation is often aimless and does not have much hope of real success. The data processing community must be made to understand that management is taking security seriously and will expect them to do the same.

Chapter 3. Security Administration Function

Establishment of the security administration function is one of the first things to be considered after direction has been defined. This chapter provides information that will help you to determine where security administration will reside and who will handle the function. This should be an initial consideration, because it is best to have the intended security administrator(s), at least those at the central level, involved with the security implementation. The administrator(s) will be better able to handle the ongoing task if they are involved from the beginning of the implementation.

3.1 Where to House Security Administration

The security administration function can live anywhere within the organization. The best place is in a security administration area that reports directly to top management. This allows the function to handle its responsibilities without the compromises that may result from loyalties to the functional area which security administration is part of. It may also be advantageous to include all security functions, including physical security activities, within this area. This follows the classic "separation of duties" approach.

Alternative Recommendations: Many organizations cannot afford the overhead, or possibly the politics, of setting up a separate security area. In this case, the security administration function should reside in an area where it will have the **power to enforce** security. This power should be granted and actively supported by the top management of the organization. The area should also have the manpower available to staff the function. Under these circumstances, the security administration function can live virtually anywhere within an organization.

Sample Locations: The classic functional areas chosen to harbor the security function include:

Systems Software:	because it is very involved with the security software itself.
Database Management/Data Administration:	because requests for access to corporate data are usually made to this area.
Operations:	because it is responsible for all processing.
Auditing:	because it is responsible for ensuring proper access to resources in accordance to policy.

Any Port in a Storm: The security function has been known to report to corporate areas as unlikely as the Tax Department or the Personnel Department. In the final analysis, the selection of the best location for the security function differs greatly among organizations and depends on the organizational and political environment available to house the function.

Note: The corporate policy or direction statement may be the best place to detail where the security administration function will reside.

3.2 Attributes of an Effective Security Administrator

After the functional area for security administration is decided, the next step is to choose the individual(s) who will handle the function. The job of a security administrator is a tough one. The security administrator must investigate every area of the data processing environment. It is also a very responsible position which requires a strong personality. Some of the characteristics you may consider in a potential security administrator are:

- knowledge of data processing resources and appropriate security requirements,
- a high degree of responsibility,
- a personality commanding respect and trust,
- good analytical and organizational skills,
- good political awareness of the environment, and
- excellent interpersonal skills.

Establish a Backup Security Administrator: It is a good idea to establish a backup position at the outset so that the function can continue if, for whatever reason, your initially selected security administrator cannot perform his duties. Many companies set up a separate security organization to support the security implementation and ongoing administration. The staff might consist of security analysts and clerical support, in addition to the actual security administrator(s).

3.3 Centralization or Decentralization

After setting up the central security administration function, you must consider whether to centralize or decentralize the security function. There is no one correct answer—only careful analysis will determine what the solution will be for your organization.

Here are some points you might consider during this decision-making process.

Centralized Security Will:

- give ***concentrated control over changes in security*** and will possibly strengthen security enforcement.
- provide ***one point*** for security administration.
- make ***policies and procedures simpler*** to develop, enforce, and monitor.
- provide a ***higher level of security*** by limiting the number and distance of individuals authorized to change security definitions.
- allow for more ***flexible reporting.***
- require ***fewer security staff members*** than would be required by a decentralized organization.

But Centralized Security Might:

- be ***less responsive*** to the user because of logical and physical distance from the user's environment.
- involve ***longer response times*** to react to maintenance requests.
- require a ***higher maintenance work load.***

Decentralized Security Will:

- allow ***more sensitivity*** to user requirements, since the administrator will be more familiar with the resources being protected and with the users than is possible at the central level.
- allow ***faster response*** to maintenance requests.
- require a ***lower administration work load*** per administrator since security maintenance will be delegated among several decentralized sites.

But Decentralized Security Might:

- require more ***complex policies and procedures.***
- provide a ***lower level of security*** since the authority to modify security definitions will be performed in many disassociated locations.
- require ***more time to implement.***
- require ***additional overhead*** at the central level to monitor the activities of the decentralized administrators.

3.3.1 Set-up/Maintenance Dependencies

In any decision regarding who is to handle security administration, you must consider the amount of setup and maintenance activity required. This activity will depend on:

- The number of corporate entities, such as departments, divisions, applications.
- The number of defined users, as well as employee turnover requirements.

- The number of data processing resources to be protected.
- The existence of standards; standards are discussed later in detail.
- The different kinds of facilities to be protected, and the extent of security required on each.
- The number of hardware entities to be protected. For example, if terminal protection is used heavily and regular network reconfiguration is a fact of life, security maintenance based on terminal ID revisions will be heavy.
- The application development activity. If heavy development is being pursued, the security requirements for maintenance activity and security review activity must be considered for new and revised application segments.
- Auditing requirements and frequency of change to them.
- The number of special routines requiring user-defined resources, and the maintenance activity against them.

3.3.2 Suggested Solutions

If maintenance activity will be fairly low, centralization might be the best approach. However, if maintenance activity is high and fragmented, decentralization may offer better and more efficient security administration.

Centralize Now, Decentralize Later: Many installations successfully use the central security administration approach and later decentralize the function wherever maintenance requirements make it practical. This is often a more sensible initial approach, since it allows the central level staff to become the security system experts before they are required to train and monitor administrators and staff on a decentralized level.

3.3.3 Administrator's Responsibility

The typical responsibilities of centralized and decentralized administrators were detailed in Chapter 2. In brief, security administrators must be responsible for implementing, maintaining, monitoring, and enforcing security and the CA-Top Secret security software.

Chapter 4. Assigning an Implementation Team

The security implementation will require concentrated effort by the assigned individual(s). It may also require cooperation and contribution from the other affected areas in the organization. For this reason, many organizations create a security implementation project team.

4.1 Suggested Team Members

The team may consist of the individuals assigned to the actual implementation and representatives from each of the following affected areas:

- Security Administration
- Systems Software
- Applications Software
- Operations
- Auditors
- End users

Cooperation is Essential: Psychologically, it is important to note that a security implementation forces cooperation between corporate areas which may never before have been forced to work together. This cooperation, critical to the successful implementation of a security product, provides yet another reason why a clearly defined management commitment to the security implementation is needed.

4.2 Project Team's Function

A security implementation is a major project. As with any major endeavor, good project management guidelines should be followed. A project manager should be assigned, regular meetings held, and an archive established of all pertinent documentation relating to this project.

4.3 Develop Security Policy

The initial assignment of the security implementation project team may be to develop and recommend the security policy or document of security objectives. The team is an ideal committee to develop this document, because the concerns of each area can be taken into account when objectives are developed. If each area agrees to the direction being set, implementation can proceed smoothly without time-consuming discord among the areas.

If the security policy or document of security objectives has already been developed, the implementation team can use this document as its mandate.

The next task to be addressed by this team is the development of the security implementation plan. Guidelines for the design of a plan are provided in Chapter 5.

Chapter 5. Developing an Implementation Plan

Planning and scheduling the security implementation can help set proper direction and keep the implementation on course. This chapter provides a few guidelines for constructing a realistic schedule and briefly discusses each component of a well-crafted implementation plan.

5.1 Construct a Flexible Schedule

Timeframes can be established if the administrator has a good feel for the size of the task. But more often, the base of users and resources is an unknown quantity. It is also usually difficult to guess what will be uncovered as the implementation continues. A security administrator soon discovers that she must become generally knowledgeable of every system, application, operations procedure, and facility in the shop. This is something that is not obvious until the inventory and design phases begin.

The implementation team should draft a flexible schedule. If at all possible, avoid setting a final implementation date until the inventory and design phases are completed. Plan to take care of the emergency requirements first and then phase in the remainder of the organization. If careful planning and analysis are done up front, the implementation will progress smoothly and will speed up as the administrator becomes more familiar with CA-Top Secret, with the environment, and with the security administration function.

It is not as important to put timeframes on each phase of the implementation plan as it is to be certain that the implementation attends to all requirements.

5.2 Consider Task Dependencies

Create a task list or flowchart showing all tasks that must be accomplished to implement security at your site. This will allow you to determine which tasks must be done as part of a step-by-step procedure, and which are independent. By analyzing all requirements initially, tasks that were intended to be handled as part of later phases may easily fall into place in an earlier phase. Tasks which should be listed are outlined on the next page.

5.3 Security Plan Components

The following tasks should be included as a part of a typical security implementation plan. The considerations involved in each task are discussed in detail in the remainder of this guide.

- **Product Training**

  Time must be allocated to allow security administrator(s) to obtain training in the use of CA-Top Secret. This task is critical because misconceptions in the use of any product can lead to delays and redesign later on.

- **Installation**

  The installation of CA-Top Secret may be scheduled at any time before actual CA-Top Secret administration is required. The time required for installation is usually minimal, especially if the user has obtained the appropriate product knowledge before attempting the installation. Development of backup and recovery procedures should accompany this task, because once CA-Top Secret is installed, your installation will most likely want to use the product initially to provide some function, even if it is only the support of security administration.

- **Inventory of Resources and Users**

  The inventory phase can be one of the most time-consuming phases of the implementation. Its duration will be determined by the number of users and resources in the installation, and whether or not enforced standards are in place. The inventory can be scheduled by logical groups of users and resources, and by facility. The results can then be input to a phased implementation.

- **Naming Standards**

  This task should be scheduled to address naming standards for the elements of the CA-Top Secret Security File. For organizations that do not have resource naming standards or have inadequate naming standards, this may be an excellent time to address the development and implementation of standard resource names. The existence of standard resource names can expedite the implementation process and will result in a clearer, less complicated security implementation.

- **Security File Design**

  The results of the inventory should give you an organized picture of the users and resources and how they relate to each other. This input should be used in designing the Security File. It is important to schedule the time to design the file before actual administration begins. This step will simplify the maintenance effort later on.

- **Definition of Implementation Strategy**

  Each organization may choose to approach the implementation in a different manner, addressing different facilities and using different options and controls. A task should be scheduled to define and document that strategy so that a clear direction is set.

- **Definition of Violation and Reporting Strategies**

  Any security product is misused if the results it reports are not monitored. It is critical to define how violations will be logged, reported, and handled. A task should be scheduled to address this important requirement.

- **Development of Emergency and Troubleshooting Procedures**

  Problems due to misuse or malfunctioning of a security product can greatly impact your operation. Before problems occur, it is critical to schedule the time to develop emergency procedures which should help minimize the time required to diagnose and resolve specific problems.

- **Define Audit Procedures**

  Schedule a task to design audit procedures which give security administrators and auditors the necessary tools to properly audit CA-Top Secret and its use within the organization.

- **Development of Security Maintenance Procedures**

  The end of the security implementation is not the end of dealing with the security product. Changes in your environment may require changes to the security definitions. Also, upgrades in the operating system may result in upgrades to the security product itself. CA-Top Secret will also periodically upgrade and add features and facilities. Development of maintenance procedures should be scheduled early in anticipation of subsequent maintenance requirements.

- **Testing**

  A test plan should be designed to ensure that the security product is implemented and functioning as desired in the installation. You will find that testing is a function that will continue, ad infinitum, as the package is enhanced and as your use of the package evolves into more elaborate security controls. A good test procedure should be developed that will be useful long after the security implementation is complete.

- **Customization**

  This task is optional. Some organizations may find that they have a unique requirement that CA-Top Secret does not address. In this case, customization is necessary. This task should be carefully scheduled with sufficient time to properly design, implement, and test the customized routines.

- **Security Awareness Programs**

  The solidity and permanence of the security implementation will depend on the support of the user community. Support will come only if the users are properly educated in the features of the security product. This important phase may be time-consuming, but it cannot be ignored since security enforcement will ultimately come from the users.

- **Ongoing Assessment and Evaluation**

  Since an implementation of a security product is as dynamic as the environment in which the product lives, ongoing assessment and evaluation programs should be developed and scheduled at regular intervals. This practice will ensure that CA-Top Secret is being used properly and effectively.

Chapter 6. Product Training

CA-Top Secret offers many controls and features, and it is important to get very familiar with what CA-Top Secret can do for you and how you can expect it to behave. A security product is not like normal system software which, after installation, performs a set system function. Although CA-Top Secret is system software and must be installed in a critical area of the operating system, it is actually an application. You must study its many functions and design an application for your own environment.

You cannot know CA-Top Secret too well. Extensive study of CA-Top Secret capabilities is a worthwhile and necessary investment of time. This study should begin before you start to plan your implementation, so that you can develop your plans based on the features and design methodologies unique to CA-Top Secret.

6.1 Learn the Basics

You should become familiar with the following information:

1. Installation. How CA-Top Secret interfaces with the operating system.
2. Default operation. How CA-Top Secret behaves by default.
3. Control options. The different options available to change the way CA-Top Secret functions. These include options in the following areas:
   a. Security System Logic Options
   b. Security State of Awareness Options
   c. Support of Multiple System Facilities Options
4. System architecture. The basic operational design.
5. Security administration functions as provided by facility and by limiting scope.
6. CA-Top Secret implementation strategies.
7. Auditing functions.
8. Logging and reporting functions.
9. Automated backup functions.

10. Recovery functions. What to do when CA-Top Secret is not operating properly. The following questions should be also considered:
    a. How will CA-Top Secret tell you that it is not operating properly?
    b. What will CA-Top Secret do when it is down?
    c. Under which circumstances will CA-Top Secret stop operating?
    d. What kind of security is available if CA-Top Secret is not operating properly?

Knowledge is Power: Know CA-Top Secret as thoroughly as possible. It is not uncommon for an unsuspecting administrator to become embarrassed when a feature (not a bug) comes to the surface when it is least expected.

In this case, knowledge is power. If you know the product well, you can control how it will behave and it will work for you. If you do not, you run the risk of being in a situation where it will control you, and this is certainly not the intent of installing a security product.

CA-Top Secret is designed to be a powerful and flexible tool for your use in enforcing security. It is not designed to tie your hands. But if you do not take the time to understand the software and how it can best be used, it can potentially work against you and you may find yourself in a situation that may take considerable time and effort to reverse.

6.2 Sources of Product Information

The following sections detail the best sources of product information.

6.2.1 Documentation

The CA-Top Secret documentation is the place to begin product training. This documentation was designed so that the set of manuals address the requirements of installation, the implementation phases, and ongoing maintenance. What follows is a listing of the various guides in the documentation set.

Orientation and Installation Materials: The orientation and installation materials should be the first ones read by the security administrator. The following guides should be carefully read and understood, because these guides lay the groundwork for successful use of CA-Top Secret in any installation.

User Guide, Part 1

Conceptual overview of CA-Top Secret architecture and capabilities.

Planning Guide

General guide for planning a successful CA-Top Secret security implementation.

Installation: Base System

CA-Top Secret installation for VSE only. (Interface installation is detailed in the appropriate facility guide.) This guide includes:

- Installation and maintenance steps
- Startup and shutdown considerations
- Backup and recovery procedures
- TSSMAINT

Implementation Materials: Part 2 of the *User Guide* should be read after the *Installation Guide* and before reviewing any of the specific facilities guides. Here you will find implementation considerations that span all facilities, including information on:

- Implementation how to's
- Application Interface
- Customization instructions

Information regarding the CICS facility appears in a separate guide:

Implementation: CICS

The facility-specific guides contain information on:

- Activating the interface
- Special control option requirements
- Implementation considerations
- Customization considerations
- Advanced techniques or applications

Auditing and Maintenance Materials: The auditing and maintenance materials contain the following:

Report and Tracking Guide
This guide details the use of TSSUTIL, TSSTRACK, TSSAUDIT, TSSCHART, and TSSCFILE. Report samples are included.

Troubleshooting Guide
This guide includes:

- CA-Top Secret debugging options and facilities,
- information needed before contacting support,
- customer support procedures, and
- the customer support system.

Reference Materials: The user should become familiar with each part of the reference materials so that at any time the proper information can be quickly and easily located. These materials are designed to assist in the day-to-day administration and maintenance of CA-Top Secret security software. The materials contain:

Control Options Guide
This guide is a comprehensive reference guide to CA-Top Secret control options.

Command Functions Guide
This guide is a comprehensive reference to the TSS command and the CA-Top Secret security panels.

Messages and Codes Guide
All CA-Top Secret messages and codes are consolidated in this document.

6.2.2 Training

Computer Associates offers formal training seminars in the use of CA-Top Secret. These seminars are developed and conducted by security professionals. The seminars include implementation strategies, advanced techniques, and auditing capabilities.

Contact Computer Associates for brochures, descriptions, and schedules of available seminars.

6.2.3 CA-World

Special sessions regarding CA-Top Secret are held at the Computer Associates annual international user conference—CA-World. These sessions provide an excellent opportunity to expand your knowledge and application of this product. Session speakers include experienced CA-Top Secret users, as well as CA-Top Secret staff. In addition, the conference is an opportunity to meet fellow users and share information and ideas on the use of this product by many different industries.

For more information on CA-World, see the CA website www.cai.com or contact your CA representative.

6.2.4 Local User Groups

There are user group organizations throughout the United States and internationally. These user groups meet periodically throughout the year to share ideas, and to keep in touch with Computer Associates on a more frequent basis.

For more information on CA-World, see the Computer Associates website www.cai.com or contact your CA representative. on CA-Top Secret user groups.

6.2.5 Security Organizations

An additional source of product and security training can be found through the security organizations that address the many issues faced during and after security implementations. What follows is a short list of some of the available sources.

Security Institutes: The Computer Security Institute located in Northborough, Massachusetts, and the MIS Training Institute in Farmingham, Massachusetts, offer conferences and seminars on security related subjects. They are an excellent source of current, practical, security implementation concepts and suggestions.

CA Security Consultants: Computer Associates is an excellent continuing source of information. A security consultant from a specialized staff of security professionals can be requested to work with you on a daily, weekly, or ongoing basis at less than market rates.

Periodicals and Journals: *Infosystems* has a regular column in each issue devoted to computer security. Journals such as the *Computer Security Journal*, published by CSI, *Computers and Security*, published by Elvision Press, and *Assets Protection* provide excellent reading for guidelines and new ideas concerning security implementation and administration. In addition, Computer Associates provides a quarterly newsletter—*The Security and Audit News*—which provides information pertaining to CA security products, future releases, and implementation strategies.

Chapter 7. Password Controls and Standards

Passwords control access to user accounts in your organization. In fact, unless you have invested in devices to provide additional levels of user authentication (for example, voice or image recognition devices, signature analysis equipment, etc.), user passwords are the only means of providing user account protection for your environment. Even if you plan to use additional user authentication devices, you should carefully consider your options for passwords and plan to incorporate the selected password options into your operation.

After you have completed product training and are familiar with the extensive controls that CA-Top Secret provides for password administration, you should begin to develop your strategies for password usage. These strategies should include a combination of password controls at the organization level (through the password control options) and at the user level (through user ACID attributes). You should also be aware of the required password controls built into CA-Top Secret which will affect your password strategy.

7.1 Rules for New Passwords

The NEWPW option defines the new password rules that will be applied to passwords installation-wide. The options available for new passwords include content or pattern restrictions, minimum length, and minimum number of days between password changes. Review the *Control Options Guide* to select the options desired by your organization.

7.1.1 Random Password Generation

This option allows you to select random password generation so that it may be selected for use through the RNDPW suboption of the FACILITY control option for any selected facility. The random password feature is often used in environments where it is important that passwords not be easily guessed.

Drawbacks to this feature are:

- When generated, the random password is displayed on the user's screen and may be viewed if the terminal screen is not protected from casual viewing.
- The randomly generated password is often not easily memorized. Thus the user might find it necessary to write it down and thereby compromise security.

It is recommended that if you use the random password feature, password masking be used to create a password that is potentially pronounceable. This might help the user to remember the password without writing it down.

7.1.2 Prevent Password Changing

The NEWPW option also allows you to prevent users from changing their own passwords. The potential problems resulting from selecting the NU suboption are:

- The CA-Top Secret security administrator must change all user passwords at the interval specified for each user (see the section "Password Attribute For ACIDs" later in this chapter).
- The revised passwords must be communicated to the users at the specified intervals, risking regular compromise of password confidentiality.
- If you choose to suppress password change intervals, password guessing has a greater chance of success because the user's password will never change.

If you decide to prevent users from changing their own passwords and you enforce password change intervals for user ACIDs, you should develop a secure procedure for communicating passwords to your user community to ensure that only the appropriate user is receiving his own password.

7.2 Honoring Passwords for Batch Jobs

The Honor Previous Batch Password option (HPBPW) selects a number of days that CA-Top Secret will honor an immediately previous or expired password for batch jobs. This allows batch jobs that execute the next day, or any selected number of days after they are submitted, to execute without abending due to expired or incorrect passwords. By default, this option is inactive.

Exposure: There is an exposure in using HPBPW, in that normal expired password control or current password entry requirements are not in effect for batch jobs for the length of time specified by this option. Also, if a user suspects that his password is known and changes the password, the previous password will still remain valid for batch jobs for the length of time specified by this option.

Recommendation: You may wish to use this option, particularly if delayed batch processing is normal in your organization. However, if used, it is recommended that the length of time specified for this option be set as short as possible.

7.3 Inactive ACIDs

The INACTIVE option defines the number of days before CA-Top Secret will deny use of an ACID with an expired password. This option is not active by default.

Recommendation: It is recommended that this option be used if you wish to deter use of ACIDs with expired passwords. You should set the inactivity threshold high enough to allow normal periods of inactivity, such as vacations, and low enough to limit exposure from employees who have transferred or terminated. The inactivity threshold is most often set at 30 days.

7.4 Password Violation

The PTHRESH option sets a password violation threshold which, when exceeded, will suspend the user. The threshold count begins from the last successful signon. The default threshold is three password violations. You may wish to revise this option. However, as you increase the threshold, password guessing by unauthorized users has a greater chance of success.

7.5 Restricted Password List

The RPW option allows you to modify the restricted password list and lets you prevent your users from entering new passwords prefixed with entries from this list (RS suboption of the NEWPW control option). For example, you can add additional restrictions to this list. You may wish to include prefixes specific to your organization, such as corporate names or acronyms. The use of this option can further restrict attempts at password guessing by unauthorized individuals by restricting passwords which may be common to your organization.

7.6 Password Attribute for ACIDs

Use of password controls can be further refined by using the PASSWORD attribute on each user ACID. The available options are:

Parameter	Description
password	You can select a password for a user ACID to be used the next time the user signs on.
NOPW	You can specify that an ACID does not require a password. It is recommended that this absence of control be used only when necessary. It should never be used for ACIDs that have access to online facilities. ACID names are often commonly known in an organization, and an ACID with the no password attribute (NOPW) is virtually unprotected.
interval	You can specify the interval at which a password must be revised. The user will be forced to change his password at the defined interval. If you have decided not to allow the user to change his own password, the CA-Top Secret security administrator must replace the password before or when the password expires, or the user's ACID will become unusable. If no interval is specified, the default interval is the value set through the PWEXP control option.
EXPIRE	This parameter, used when creating a password for the first time or when replacing a password, will expire the password the first time the associated ACID is used. This is used most often to establish and encourage confidentiality of passwords as quickly as possible. It is recommended that organizations choosing to allow users to change their own passwords use this parameter whenever passwords are created or replaced so that even the administrator will not know what the password is after the user first uses the ACID.

Review the *Command Functions* guide for details on the syntax of, and requirements for, the PASSWORD attribute.

7.7 Setting a Password Expiration Interval

The PWEXP control option allows a site to specify a password expiration interval which, in effect, becomes the default interval for the installation. Changing the expiration interval would have no effect on current users, only on those who have been created after the change.

7.8 Suppressing Password Viewing

The PWVIEW control option allows a site to suppress the viewing of users' passwords. If set to YES, PWVIEW allows the display of passwords if the administrator has the PWVIEW authority level specified in the DATA parameter of the TSS ADMIN command function.

7.9 Maintaining Password History

The PWHIST control option allows a site to maintain a password history for users by specifying how many passwords should be retained in history. Up to 64 passwords can be specified. When used with the many existing password control options, an installation can easily ensure that users do not regularly reuse common passwords.

7.10 Conclusion

A word of caution: do not develop password requirements before you have studied the options available with CA-Top Secret. There are organizations that have invested much time in developing password requirements only to discover that these requirements cannot be handled by the security product without customization. Conversely, you may run the risk of inadequate controls based on incomplete knowledge of the extent of password controls available to you with CA-Top Secret.

Chapter 8. Installation

The installation of CA-Top Secret security software is trivial in comparison with the installation of most software products. CA-Top Secret installation does not require the coding of VSE system exits, and, most importantly, modifications to operating system code.

If you have had experience with software product installations, you should be able to install CA-Top Secret in less than one hour. Installation may take a little longer if you have never installed software before. Installation steps are detailed in the *Installation and Maintenance* guide.

8.1 Prerequisite Information

Before installing CA-Top Secret, you should read:

- *User Guide*
- *Installation Guide*
- *Control Options Guide*, and of course
- this *Planning Guide*

8.2 Select Control Options

CA-Top Secret control options detail CA-Top Secret operation in specific circumstances. It is a worthwhile investment of time to study the control options and their defaults before installation.

It is important to understand how CA-Top Secret will behave even if you choose to install CA-Top Secret with default control options. In most cases, you will choose to alter some of the defaults when you first install CA-Top Secret.

The control options detailed next should be given special consideration before installation. These options generally affect CA-Top Secret operation and should be reviewed for default operation.

Option	Description
AUTH	The AUTH control option controls the method of search in the CA-TOP SECRET authorization algorithm. Once you have chosen the setting for this option and have begun your implementation, this control option should not be changed because you will then change how your CA-Top Secret definitions are searched. If changed, this may result in valid access against resources that were thought to be restricted. Careful thought should go into the setting of this option. The default setting—(OVERRIDE,ALLOVER)—is recommended.
BACKUP	This option controls the CA-Top Secret automatic backup feature. By default, CA-Top Secret automatically takes a DASD backup of the main Security File at 1:00 a.m. as long as the backup file is defined in the CA-Top Secret started task. It is recommended that you use the automatic backup feature to allow for quick recovery of the Security File.
DATE	This control option lets you format dates for report and display purposes. Although this option can be changed at any time, you might wish to set this option in the format most accepted in your environment before installation to avoid confusion when CA-Top Secret begins to display messages. CA-Top Secret has been fully prepared for Year 2000. Years between 80 and 99 are presumed to be in the twentieth century. Years outside this range are assumed to be in the twenty-first century.
DOWN	The DOWN control option controls security for tasks initiating while CA-Top Secret is down. The default allows started tasks to bypass security, but all other tasks must wait until CA-Top Secret has been restarted. The DOWN option takes effect in all modes except DORMANT mode. Although you may not choose to change this setting, it is important to note that this is the way that CA-Top Secret behaves when the CA-Top Secret address space is inactive.
MODE	By default, CA-Top Secret initializes in FAIL mode. You might wish to change this at installation to DORMANT mode so that you can begin to use the TSS command to do administration without affecting your ongoing operation. DORMANT mode is the first phase in a gradual CA-Top Secret implementation.
RECOVER	This control option indicates if the CA-Top Secret Recovery File is being used. CA-Top Secret assumes that the Recovery File is being used if it is included in the CA-Top Secret started task procedure. Include the Recovery File in the CA-Top Secret started task procedure if you intend to use the CA-Top Secret Security File recovery procedure, or if you wish to track Security File administrative activity using the TSSAUDIT utility.

8.3 Installation

After you have selected your startup control options, you are ready to install CA-Top Secret. It is recommended, as with any product that interacts with critical system operations, that you not install during peak production periods. However, as long as you have set the MODE control option to DORMANT, CA-Top Secret will not impact your operation after installation, but will give you the capability to use the TSS command for security administration.

Follow the *Installation Guide* carefully throughout installation and use the installation checklist. This will ensure a smooth installation.

Chapter 9. Backup and Recovery Procedures

Once CA-Top Secret is installed, you should consider developing security file backup and recovery procedures before you begin CA-Top Secret administration. This will ensure that your security definitions can be recovered from day one of your implementation.

9.1 Security File Backup

Of course, the most critical file is the Security File itself. CA-Top Secret has an automatic backup feature that is set to copy the Security File to a DASD backup at 1:00 a.m. daily. This Backup File is critical to the built-in recovery capability. You can change the time of backup or deactivate the automatic backup through the BACKUP control option. Also, a backup can be taken at any time from the console using the BACKUP modify command. Review the *Control Options Guide* for the use and syntax of the BACKUP control option.

9.2 Recovery Procedure

CA-Top Secret also includes a recovery mechanism based on the DASD backup and the Recovery File. This procedure should be installed and tested before serious security maintenance begins so that all Security File updates can be recovered. Details on the CA-Top Secret backup and recovery routines are included in the *Installation Guide*

It is recommended that you use the CA-Top Secret backup and recovery procedures to protect your CA-Top Secret Security File. These procedures were designed for quick, accurate, and dependable recovery.

9.2.1 Training Operators

When setting up the backup and recovery procedures, you should also take time to train key operations personnel in the use of the backup and recovery routines, so that they are prepared to execute them when necessary. Emergencies do not present the appropriate opportunity for training.

9.2.2 Candidates for Offsite Storage

As with all critical files used in your installation, all of the CA-Top Secret files including the:

- Security File
- Security File backup
- Recovery File
- Audit/Tracking File
- CPF Recovery File
- Parameter File

should be backed up to tape or cartridge daily, and should be candidates for offsite storage. Offsite storage will protect these files if your data center experiences a major disaster.

It is also recommended that the Security File reside on a different volume and string than that of the Backup and Recovery Files. This will allow you to use the Backup and Recovery files to quickly and easily circumvent minor hardware problems which affect access to the Security File.

Chapter 10. Resource/User Inventory and Exposure Analysis

This is often the first time that most organizations have taken an analytical look at the kinds of data processing resources they own and all of the individuals who access those resources (whether or not they actually need to have access). A user and resource inventory and exposure analysis is usually an enormous task, often too large to be handled all at once. For this reason, many organizations address the analysis on a user group basis, targeting implementation a group at a time. In fact, it is often helpful to solicit the support of the various user groups in doing the inventory, since each group will be the best source of information on the resources required for their own needs.

It is recommended, if the size or complexity of your organization warrants, that you address the inventory in manageable segments. Additionally, you may wish to further segment the effort by facility, since the nature of the resources differs among facilities.

Note: You should be aware of the different resource types used in each facility and should carefully determine appropriate controls on each resource type.

This chapter provides guidelines for this analysis and introduces several tools which make the task easier and more effective.

10.1 Objectives of the Inventory

The inventory and exposure analysis should answer the following questions:

1. Who are the users?
2. What are the resources? Must they be classified?
3. Who is responsible for the resources?
4. Which users are accessing which resources?
5. Which users must access which resources to accomplish their job function, and at which access level?
6. Which operations and procedures leave critical resources exposed?

10.2 Prioritize Users, Resources, and Facilities

You should prioritize the facilities to be protected, the users to be defined, and the resources to be protected. This will allow you to implement security for the most critical facilities, users, and resources first. As each inventory phase is completed, you should input the results into your Security File design and implementation strategy before continuing with the next inventory phase.

Note that inventory information is dated. Since environments change and grow quickly, you may have to reanalyze the segment if you do not quickly implement the results of your research.

10.3 Organize Users into Groups

Group the users together by corporate entity and job function. This organization may have already been accomplished for you as part of VSE subsystem assignment, such as the standard CICS or additional facility user tables. The results of the user inventory will be input to the department and division design discussed in Chapter 12.

10.4 Take Inventory of Resources

Use existing automated records of resources that already exist in your site, such as:

- JCL libraries, VTOC listings, and audit information for data sets and volumes.
- Load library directories for programs.
- CICS tables for CICS resources.
- VTAM tables for available terminals.

10.5 Organize Resources

Detail each resource or set of resources as to:

- the type of resource,
- who owns or is responsible for the resource,
- where the resource is recorded, and
- the purpose of the resource.

Remember that CA-Top Secret supports data set masking as well as full resource prefixing, so you may not have to detail each resource specifically if you can easily detail a resource group by masking or prefixing.

10.6 Assign Access Levels to Users/Resources

After you have decided which resources are candidates for protection, you can assign these resources to the appropriate user group at the appropriate access level. This information will be specific input to resource ownership decisions and design of profiles which you will perform in Chapter 12.

Record Assignments Online: Recording your inventory results in an automated fashion, possibly using an online editor such as ICCF, may serve you in later converting this information into the required TSS commands. In fact, it will save you time to record the results of your inventory in TSS command format. The results can then be easily revised for last-minute adjustments and can be directly input to the batch utility to update the CA-Top Secret Security File. It is important that this inventory be carefully restricted to avoid security pilferage or tampering.

Sample inventory results for a set of fictional batch and CICS resources appear in Appendix B. You may wish to organize your inventory in a similar fashion.

10.7 Conclusion

Whichever approach is taken, the inventory is a vital step in protecting your organization's resources. You cannot protect an environment until you have identified and accurately described that environment.

Chapter 11. Developing Naming Standards

Naming standards are the sort of thing that everyone sees the need for but no one wants to develop or enforce. If your organization has successfully designed and enforced standards prior to the security implementation, your implementation will be much easier since you will be able to use CA-Top Secret's resource prefixing or masking capabilities to define resources. This will relieve you from having to define each individual resource by allowing you to group resources together by prefix or pattern.

However, if you are implementing security in an organization that has not enforced standards, or if you have no set standards at all, your implementation will be somewhat more complicated. You will have to create more resource definitions, or you may wish to alter your current naming standards.

11.1 Resource Naming Standards

Once the resource/user inventory has been completed, and you have a good feel for what resources the organization owns, and who is responsible for them, you can design standards or seriously plan to enforce the standards that were designed but never used successfully. CA-Top Secret can be used to allow users to read or update resources that currently exist, and which do not follow the standard, but not allow users to create resources that do not follow the standard.

11.2 User Naming Standards

CA-Top Secret implementation is also a good time to review your user ID naming standards. Many installations find that they have used different standards for each facility. For example, the user ID in ICCF, which is restricted to four characters, may not be the same as the CICS signon name. Some organizations find that they have generated user names randomly, without following any predefined standard.

Since CA-Top Secret (without customization) uses a user ID of eight characters because the ACID is restricted to eight characters, you may wish to reevaluate your user ID standards. It is a good idea to use one user ID (ACID) across facilities, so that a single identifier can identify a user no matter which facility she is using.

11.2.1 Common Naming Standards

There are many theories on the development of user IDs. Some of the more common are discussed next.

Unique User IDs: The user ID can be unique to the user. Although generic ACIDs—those that allow more than one user to use the same ACID at the same time—are supported with CA-Top Secret, it is recommended that each user be assigned a unique ACID to establish accountability for the use of the ACID. This allows you to trace violations and audited events back to the correct individual.

It is also recommended that this ACID not be reused when the user transfers to another department or terminates employment. This will allow you to trace the events associated with this user historically.

Static User IDs: The user ID can remain unchanged for the user's full term of employment, even if the user transfers to a different department. The type of ACID usually chosen to follow this theory is a unique ACID which identifies the employee, such as employee name or number.

Dynamic User IDs: The opposite of the preceding approach is to choose an ACID which identifies the department or location of the user by ACID prefix and identifies the user with a unique ACID suffix. This type of ACID will be changed when the user transfers to another department, because the prefix of the ACID determines the department and the general responsibilities of the user. This type of ACID allows security administrators and even computer operators to quickly determine when, for example, a user outside of the Payroll Department is attempting to access a payroll resource.

Secret IDs: A common theory is to obscure the user ID so that it cannot be easily guessed by an interested third party. While this can be an effective measure to deter unauthorized users from getting into unauthorized accounts, it can be very difficult to administer, since it will be just as difficult for the administrator to determine the owner of the ACID without listing the ACID from the CA-Top Secret Security File. This can make auditing and violation monitoring more difficult. Although this is an often-used and viable approach, it might be better to depend on strong password controls and possibly user authentication devices to deter unauthorized access to accounts without obscuring the user ID.

Whichever standards you choose to follow, it is recommended that you determine your approach before you begin to build your Security File and define your users.

11.2.2 CA-Top Secret Security File Standards

CA-Top Secret uses ACIDs to define the functional entities within the Security File. The ACID names used in the file should also follow a standard, to simplify maintenance and to allow the definitions to be readily located for research and analysis. For example, you should be able to determine by the ACID name if the ACID is a user, a profile, a department, a division, a zone, or a CA-Top Secret security administrator.

Chapter 12. Designing a Security File

Given the results of the user and resource inventory, and after studying the features available with CA-Top Secret, you can design your CA-Top Secret Security File. The design of your Security File is most effective if you use both your environment and CA-Top Secret's capabilities as input. The following sections discuss the steps necessary to effectively design the Security File.

12.1 General Guidelines

There are a few general guidelines to keep in mind when designing the Security File.

- Keep the file structure simple. The structure can follow your organization's functional areas of responsibility.
- Standardize the Security File names as discussed earlier in Chapter 11.
- Use a consistent approach and style in designing the file. Remember that you are designing a file just as you would for any application and that it is best to keep it simple, straightforward, and understandable.

These techniques will simplify maintenance and help you find a file element quickly when you need it.

12.2 Security File Structure

Most organizations base the CA-Top Secret Security File structure on their corporate organizational structure. Each organizational group that requires access to mainframe resources should be defined as a department or division to CA-Top Secret as shown in the figure below.

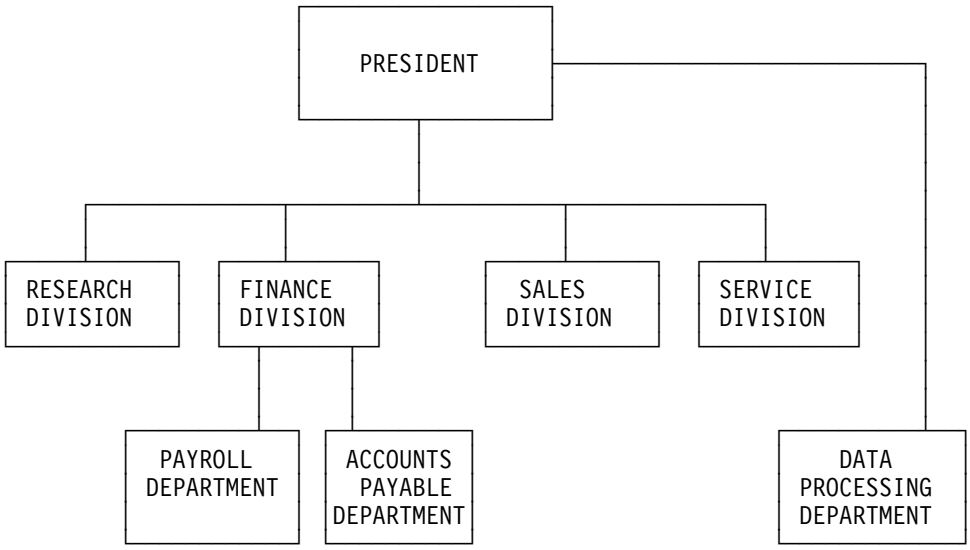


Figure 12-1. Corporate Organizational Chart

Depending on the size and structure of your organization, you may also want to group several divisions together and assign them to a zone.

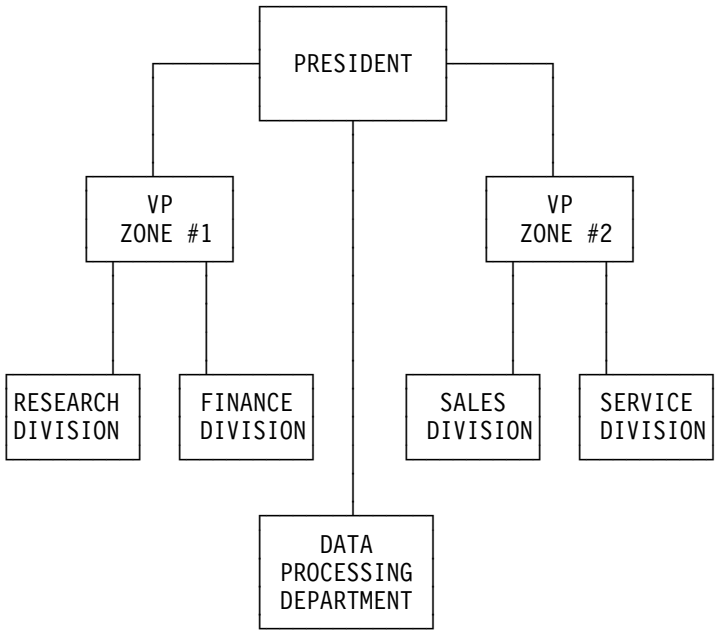


Figure 12-2. Using ZONES

12.3 Defining Department, Division, and Zone ACIDs

It is highly recommended that you take the time to design your Security File and to define this structure to CA-Top Secret. The CA-Top Secret departments, divisions, and zones give you a reference point on which to establish ownership based on corporate responsibility, and also give you a logical grouping of users based on their position within the organization as shown in the next figure. Even if you initially choose to centralize security, you will be able to easily respond to decentralization requirements when they arise for administration, auditing, or reporting purposes.

Note: Use of division and zone grouping is optional.

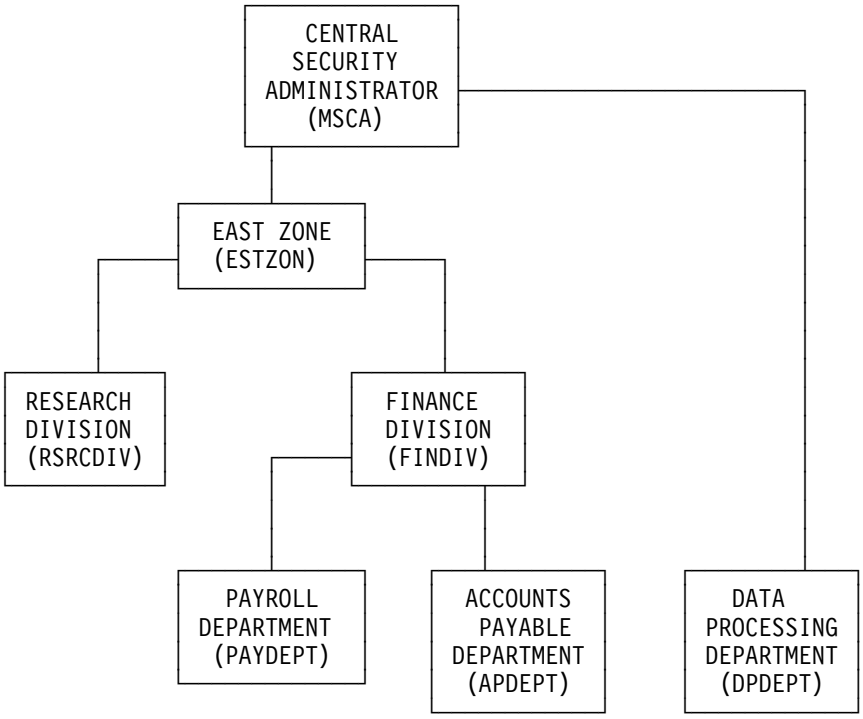


Figure 12-3. Defining DEPARTMENTs, DIVISIONs, and ZONEs

12.3.1 Organization ACIDs Provide Structure

It is not necessary to have a one-to-one relationship between the zones, divisions, and departments in your organization and CA-Top Secret zones, divisions, and departments. These organizational ACIDs are provided to form structure and scope within your file. The CA-Top Secret terms zone, division, and department in no way indicate that these entities must equate to actual zones, divisions, and departments. Think of these ACIDs as providing levels of control.

Examples: In a large sales-oriented company, CA-Top Secret zones may be used to differentiate the Research and Marketing Divisions in the East coast office from the same divisions in the West coast office. In a service company, CA-Top Secret divisions may represent client companies. In a small organization, CA-Top Secret divisions may represent corporate departments and CA-Top Secret departments may represent units within each department. In some organizations, it might make sense to mix the use of zones, divisions, and departments to resolve the unique requirements of different corporate entities.

12.3.2 Do Not Delay File Design

It is often tempting to ignore designing a file structure as a first step in creating the CA-Top Secret Security File. Some organizations have overlooked this first step and have begun to define ownership and users within one large department without taking the time to analyze and design the breakdown of access requirements as they relate to the organizational chart. They later find themselves creating an ad hoc structure to respond to special decentralization requirements which results in a file design without any real structure or forethought. This can become a maintenance nightmare.

12.4 Defining Resource Ownership

After you have done your resource inventory and have established corporate responsibility for your resources, you can plan to define ownership of resources to the selected corporate entity (department, division, or zone). It is highly recommended that ownership be defined at this level for two reasons.

1. Ownership of resources at the user or profile level equates to default access levels that cannot be overridden. Therefore, fine tuning of access requirements for a specific resource cannot be done for the user or profile that owns the resource. Ownership at the department, division, or zone level does not equate to any default access for the users defined within that department, division, or zone.
2. If ownership is defined at the user level, ownership must be transferred to another ACID if the user terminates. This can become a maintenance problem.

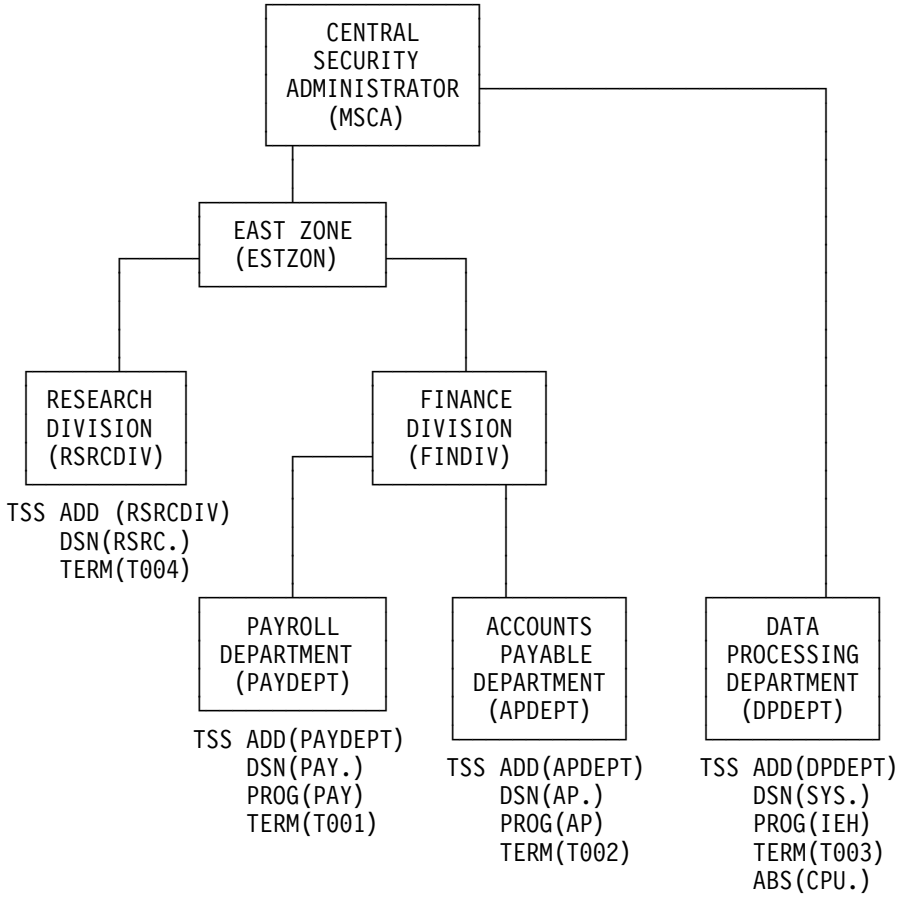


Figure 12-4. Define Resource Ownership

12.4.1 Defining Ownership to Users

Ownership of a user's own scratch pad data sets (for example, II user ID data sets) is a situation where it might be useful to define ownership at the user level. This approach can help to enforce cleanup of work data sets as well as CA-Top Secret Security File definitions when an employee terminates. Of course, ownership of a user's personal data sets can still be defined at the department, division, or zone level if desired.

Ownership at the profile level is **not** recommended.

12.4.2 Defining Ownership to Master Security Administrators

There are special cases when it is recommended that ownership be defined to the MSCA. These cases include ownership of MODEs and ownership of prefixes which include masking characters. The *User Guide* discusses requirements for ownership at this level.

12.4.3 Defining Ownership at High-Level Prefix

When establishing ownership of resources, plan to define ownership at as high a level (as short a prefix) as possible. For example, for data sets, try to define ownership by the high level prefix; for programs, by program prefix. This will simplify and reduce the number of required CA-Top Secret ownership definitions.

For the data set name SFT1.MASTER.FILE, you should assign ownership of SFT1. not of the full data set name.

12.5 Designing Profiles

Profile ACIDs are used to group together access requirements that are common to more than one user. It is recommended that careful thought be given to designing the use of profiles in your organization.

12.5.1 Defining Job Requirements

The most common and recommended use of profiles is to define job position requirements in access definitions. These requirements can be defined in one profile or in a series of related profiles. Use the results of your resource inventory that detail which users require access to which groups of resources as input to your profile design.

12.5.2 Designing Options

Consider the options discussed in the following sections in designing your use of profiles.

12.5.2.1 Attaching Profiles to Departments

You can design your profiles so all users assigned to a department are attached to profiles which are attached to that same department. Profiles MUST be attached to departments.

Example 1: The Application Department requires access to system resources. PROFILEX, which is attached to the Application Department, contains the access requirements for the system resources. Therefore, to allow all Application Department users to access system resources, you would attach PROFILEX to the user ACID of each user via a TSS ADD or CREATE command.

You can also design your profiles so the profiles attached to a department define access to resources that are owned within that department. Users in **any** department who require access to these resources can then be attached to these profiles.

Example 2: PROFILEZ, which is attached to the *Systems* Department, contains the access requirements for the system resources used by the *Application* Department users. To allow Application Department users to access the systems resources, you would simply attach them to PROFILEZ via an ADD or CREATE command.

Example 3: The next figure shows a sample profile design organized by departments.

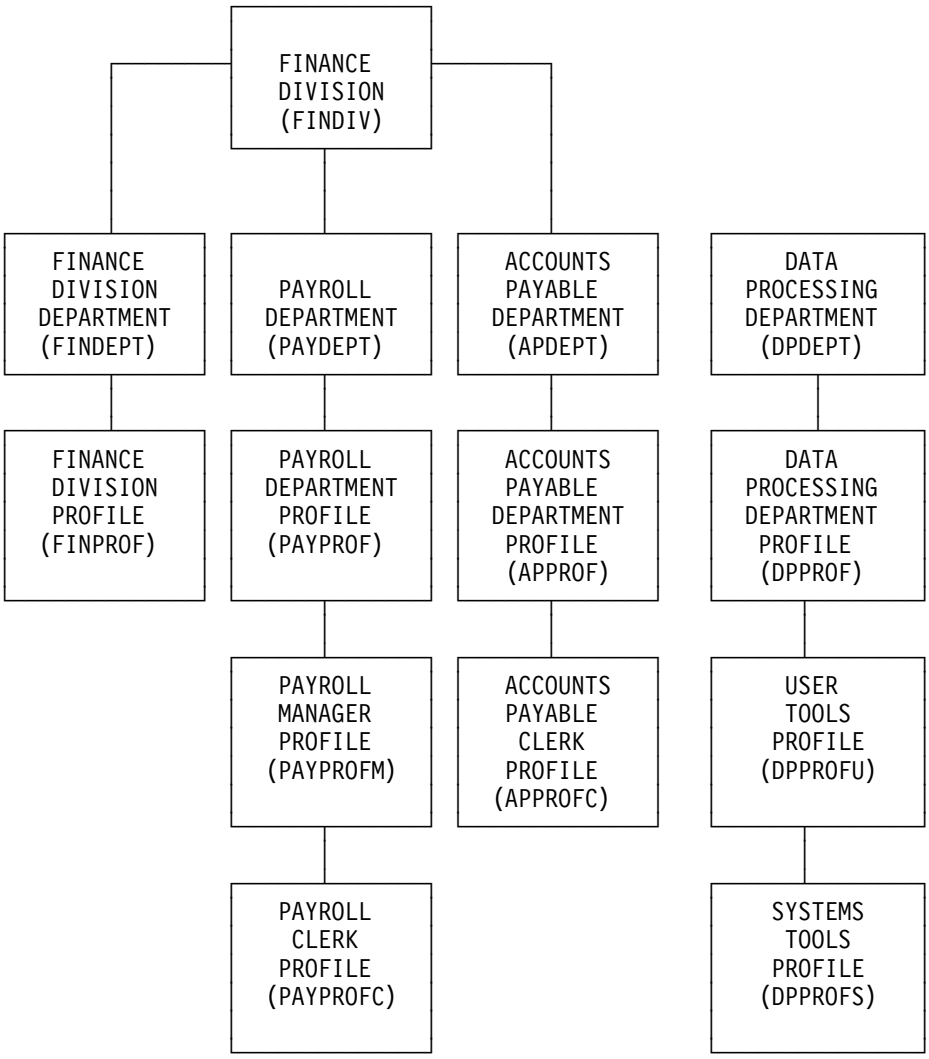


Figure 12-5. Profile Design

12.5.2.2 Department/Division and Department/Zone Level Profiles

In addition to job description profiles, it is a good idea to design department and division (optional) level profiles for each user. Even if you initially do not have department or division level requirements, you should attach these profiles to your users as the users are created and are associated with specific departments. When later requirements surface that affect users on the department or division level, you can fulfill these requirements simply by updating the appropriate department or division level profile.

Profiles cannot be attached to divisions or zones. To effect higher level profiles, for instance, create a divisional department to which no users will be attached, and create your divisional profile within this department.

12.5.2.3 Defining Profiles by Facility

Profiles can be defined so requirements for a given facility are defined within the profile. Batch requirements, for example, can be defined in one profile while CICS requirements are defined in another profile.

12.5.2.4 Defining Profiles by Application

The payroll CICS system requirements, for example, can be defined in one profile and the personnel CICS system requirements can be defined in another. A user requiring access to both payroll and personnel applications can be attached to both profiles.

12.5.2.5 Override Strategy

If you choose to use the default options of the AUTH control option, you can use override strategy in designing your profiles.

Example: PROFILEA can be defined to allow READ access to system data sets. PROFILEB can be defined to allow UPDATE access only to a critical subset of data sets defined by PROFILEA. A user attached to PROFILEB and PROFILEA in the following order:

1. PROFILEB
2. PROFILEA

will have UPDATE access to the critical data sets, and READ access to the remaining data sets where the access has not been overridden by PROFILEB. Additionally, other users who only require READ access to system data sets can simply be attached to PROFILEA.

12.5.2.6 Defining Profiles by Job Description

You can choose to use a single profile per job description.

Example: A payroll clerk's job will always be defined by PROFILEP while the payroll manager's job will be defined by PROFILEM. Although the payroll clerk and the payroll manager might share common access requirements, they will nonetheless have individual profiles. This approach makes it very simple to determine the access requirements for a new user assuming the job of payroll clerk or payroll manager.

Note: Profiles are still recommended even if the job description profile is only applicable to one user. When a new user assumes that job position, you can simply attach the profile or series of profiles to the new user, eliminating the need to redefine all of the required access definitions for that user.

12.5.2.7 Number of Profiles

The number of profiles that you can define for your organization is unlimited. The number of profiles that you can attach to each user is limited to 254. However, it is recommended that you limit the number of profiles attached to each user as much as possible. If your use of profiles is carefully designed, you should not require more than five or six profiles per user.

12.6 Recording All Universal Access Requirements

The ALL record is used to record all access requirements which will be effective for all users, both defined and undefined, to CA-Top Secret. The ALL record is a powerful implementation tool which allows you to protect and define resources, but still allows undefined users to access those resources at a specific level as defined to the ALL record.

Your Security File design for FAIL mode, when all users are defined to CA-Top Secret, should indicate limited use of the ALL record. Only truly global requirements should be defined to the ALL record. For example, use of the corporate phone number application or electronic mail system might legitimately be defined in the ALL record.

12.7 Defining Users

The results of the user inventory are input to the creation of users. It is often painful to postpone defining users until the Security File design has developed to this point. However, the existence of departments in which to define users and the existence of profiles to define access requirements for the users will greatly simplify the actual definition of users to CA-Top Secret.

At this point, creating users is a rote exercise, since all the pieces are in place to describe the proper environment for each user. But this is, of course, the point at which your users will be able to sign on under CA-Top Secret control—which is the goal of the security implementation. You have designed your Security File well if you find that creating users is a simple and straightforward task.

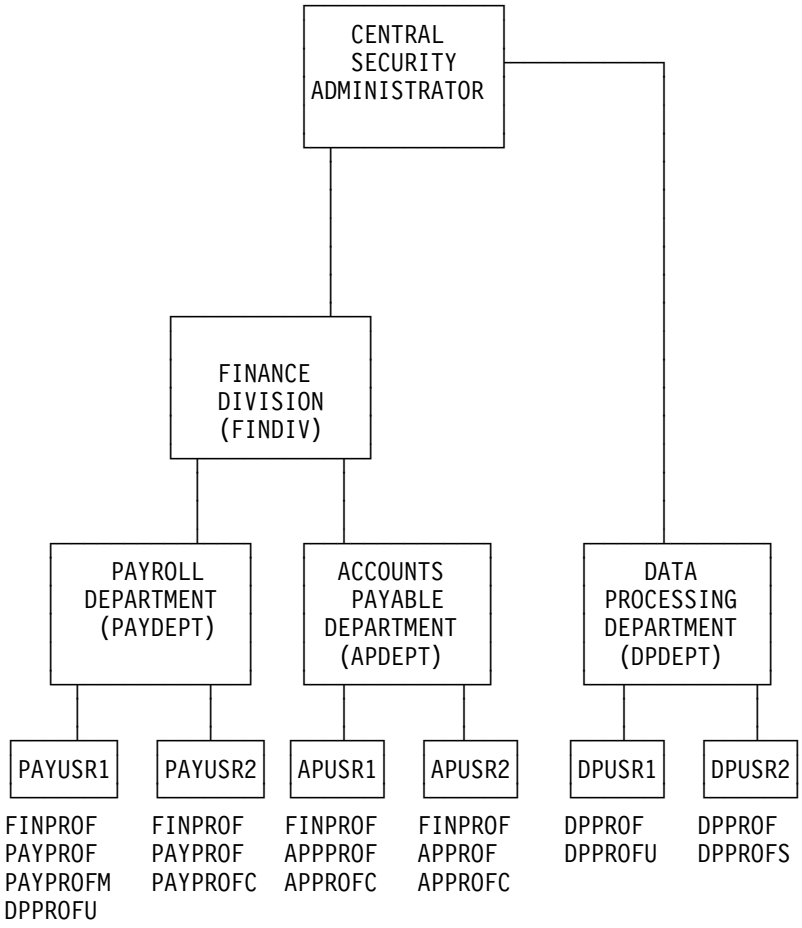


Figure 12-6. Defining Users

12.8 Defining CA-Top Secret Security Administrators

CA-Top Secret security administrators are special kinds of users and must also be incorporated into your Security File design. Chapter 13 discusses refining your security administration requirements.

12.9 Documenting Security File Design

It is a good idea to document your Security File design, and what you have intended with its design and approach.

12.9.1 ACID Description

The NAME field of the TSS CREATE command provides a descriptive area for each ACID. This field allows for a 32-character description of the ACID. You may find that this is not enough space for a meaningful description, particularly for profiles as described previously. It may be useful to develop a Security File dictionary that details each ACID by name, its purpose, and the nature of its use.

CA-Top Secret also provides an installation data (INSTDATA) field, which administrators may use for auxiliary security information.

You may add descriptive fields and segments to your ACID structure through the CA-Top Secret Field Descriptor Table (FDT). By adding such descriptive fields, you can store specialized information about your users beyond the 32-character limit. These fields may also be retrieved for security purposes.

12.9.2 Viewing Your Security File Organization

TSSCHART is a useful utility when used to document your Security File design. It will flowchart the organization of your Security File at any level, and will indicate the levels at which resource ownership is defined. TSSCHART is an effective review tool as well as a documentation tool. You may wish to use this utility throughout implementation to ascertain that the actual file design is following your original plan. TSSCHART is discussed further in the *Report and Tracking Guide.*

Chapter 13. Refining the Security Administration Structure

The task of creating, maintaining, and monitoring the CA-TOP Secret Security File falls to the CA-Top Secret security administrators. There are many CA-Top Secret options available to handle your security administration requirements. Therefore, some thought should be given to designing the CA-Top Secret security administration function for your organization.

Chapter 3 discussed considerations for setting up your security organization. By this time, your plans for this organization and tentative plans for decentralization, if desired, should be defined.

Who Administrates Security? Minimally, a central level individual should be responsible for CA-Top Secret Security File creation and maintenance. It is important to note that the corporate security administrator or officer does not have to be the same person as the CA-Top Secret security administrator. This is most often true in large organizations where the security administration function is handled by a security administration group headed by a security officer. In this type of situation, the CA-Top Secret administration might be handled by security analysts or, if the Security File is well-defined and simple to maintain, by security administration clerks.

13.1 TSS Command

The TSS command, which is the tool for CA-Top Secret administration, is easy to use. The administration menus available in many facilities can make administration even easier. As long as the Security File has been well designed and maintenance procedures have been clearly defined, it is not necessary for the high-powered corporate administrator to actually enter TSS commands.

13.2 The MSCA

The MSCA, or Master Security Control ACID, is created as part of the installation procedure. This is the ACID that allows you to begin to define your Security File once it has been designed. Your organization has the flexibility to incorporate any security design or control supported by CA-Top Secret, and the MSCA account is the account that you will use to initially accomplish this.

By design, the MSCA has complete administrative authority and control. You may choose to override this omnipotent authority, but the MSCA can always redefine his own authority back to complete control. It is best to leave the MSCA account omnipotent and protect its use accordingly.

13.2.1 Physically Secure the MSCA's Password and ACID

It is recommended that your security implementation strategy include plans to physically secure the MSCA's ACID and password, keeping them confidential and possibly locking them in a safe place so that they can be retrieved in an emergency. It is further recommended that the MSCA account **not** be used for routine CA-Top Secret maintenance. It should be used only when required. For example, only the MSCA can create SCAs or LSCAs, so the MSCA account must be used for this purpose.

13.2.2 Suspension of MSCA

By default, the MSCA account cannot be suspended because, if all else fails, the MSCA account can be used to handle maintenance, control option requirements, or emergency procedures. However, if you choose to make the MSCA account suspendable because you fear potential sabotage through password guessing from an outside source, you can do so through the MSUSPEND control option.

13.3 Additional Central Security Administrators

At least one SCA should be created as the ACID used to perform routine maintenance. There is no limit to the additional SCAs or LSCAs that you can create as required by your organization. The scope of an SCA is all users and resources defined within the CA-Top Secret Security File. The scope of an LSCA, which is essentially a **limited** SCA, is determined by the MSCA and can include other LSCAs. This characteristic may make an LSCA more useful in a security environment that is either decentralized or a mixture of centralized and decentralized.

13.3.1 Suggested SCA Authorities

An SCA is not required to have full administrative authority. You can tailor your use of SCAs to conform to the requirements of your organization. Consider the following when planning your use of SCAs:

- Additional SCAs may be required to perform routine maintenance. This may be true especially if you have centralized security maintenance and have heavy maintenance requirements.
- SCAs can be created with auditing capabilities to allow the auditing staff to monitor the implementation and maintenance of CA-Top Secret.
- Special purpose SCAs can be created with reduced authority to handle specific environmental requirements. For example, some organizations create an SCA with the authority to only suspend and unsuspend users. This ACID is assigned to an operator with appropriate procedures for unsuspending ACIDs which have been accidentally suspended.

As indicated, administrative authorities can be selectively assigned. For a full discussion of available authorities, see the *Command Functions Guide*

13.3.2 The LSCA Option

Like the SCA, the administrative authority of an LSCA can be tailored by the MSCA. However, unlike an SCA, the LSCAs **scope** is also subject to modification and need not extend to all CA-Top Secret defined users and resources. Consider the following example:

1. LSCA02 has authority over ZONE01 and ZONE02. LSCA03 has authority over ZONE03 and ZONE04.
2. LSCA01 has full administrative authority over LSCA02 and LSCA03.

This allows LSCA02 and LSCA03 to "function" as SCAs for their respective zones and yet subjects them to the administrative authority of LSCA01.

13.4 Decentralized Security Administrators

Decentralized security is set up through zonal (ZCAs), divisional (VCAs), and departmental (DCAs) security administrators. It is not necessary to define an administrator for every department. Decentralized administrators can be defined selectively as required.

One of the advantages to designing and implementing a Security File structure as discussed in Chapter 12 is that decentralized administrators can be assigned wherever and whenever it is appropriate. As long as your structure is well designed and ownership has been assigned along appropriate lines of corporate responsibility, creating a DCA, VCA, or a ZCA at the selected level effectively decentralizes CA-Top Secret security administration.

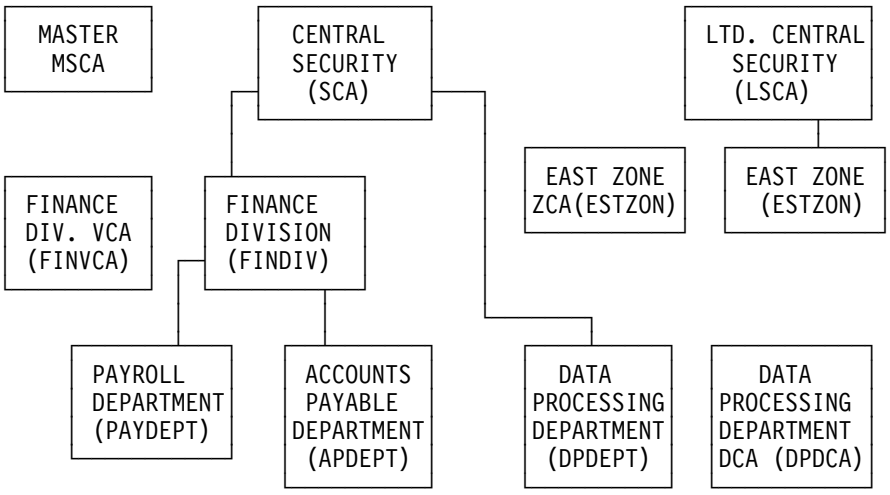


Figure 13-1. Decentralized Security Administration

13.4.1 ZCA, VCA, or DCA Considerations

Consider the following when planning to decentralize CA-Top Secret security administration:

- ZCAs, VCAs, and DCAs are most often created to perform routine maintenance.
- Temporary or permanent ZCAs, VCAs, and DCAs can be created with auditing capabilities which allow the auditing staff to perform routine or periodic audits on corporate zones, divisions, and departments.
- As with SCAs and LSCAs, special purpose ZCAs, VCAs, or DCAs can be created with reduced authority to handle specific environmental requirements.

- You can choose to assign administrative authorities to user ACIDs. For example, you may wish to allow a user to permit access to the resources that he owns to other users.

It is recommended that you decentralize administration only when and where it is necessary. Valid reasons for decentralization include heavy maintenance activity at the central level and remote user sites which require more responsive administration than can be provided at the central level. Selective decentralization where appropriate can be the most effective way of decentralizing administration.

13.4.2 Monitor Decentralization via TSSAUDIT

If you do choose to decentralize, it is recommended that you put the appropriate manual and automated controls in place to monitor the decentralized activity. The CHANGES function of TSSAUDIT can be used to regularly monitor all changes made to the Security File by administrators. This monitoring function may ultimately be assigned to the auditing staff.

13.5 Password Viewing

Administrative authorities are initially assigned by the MSCA. SCAs, LSCAs, ZCAs, VCAs, and DCAs can assign administrative authorities to CA-Top Secret administrators within their scope if they themselves possess the authorities.

The only authority that you can completely deactivate is the authority to view passwords through the TSS LIST command. This can be accomplished by setting the PWVIEW control option to NO.

It is the option of the organization to determine whether or not the ability to view passwords by even the MSCA is to be considered a security exposure and, if so, to deactivate that capability.

Chapter 14. Defining Procedures for Handling Violations

It is an important function of the security administrator to monitor the generation of violations. This chapter outlines a procedure that is often overlooked: how to handle violations when they occur and what action to take against the violator.

14.1 Monitoring to Discourage Violation Attempts

You might feel that since CA-Top Secret is stopping unauthorized access attempts, there is no need to monitor the employees incurring the violations. But a pattern of unauthorized access attempts by a user (or a related group of users) could indicate that these users are looking for a loophole in your security definitions. If they find the loophole, this **will not** show up as a violation. Therefore, a pattern of attempts might indicate a potential breach of security and should not be ignored or taken casually.

If employees sense that no one is monitoring violation attempts, they might be encouraged to try to access resources that they should not.

14.2 Elements of Procedure

If you wish to effectively discourage attempts at unauthorized access by employees and emphasize your organization's position on security, you should establish a procedure to handle excessive attempts at unauthorized access to your computer resources.

Consider the following procedure for handling excessive violations:

1. Carefully monitor your regular violation reports to determine patterns of excessive violations by specific users or groups of users.
2. If you identify suspicious users or groups of users, you might consider doing further research on access patterns by auditing the suspected ACIDs.
3. Use TSSUTIL to produce regular reports on these users, showing violations and all audited activity.
4. To monitor activity more closely, you can use TSSTRACK to monitor the suspected users as they are working, and later produce reports on your observations.
5. If the attempts are made against a specific set of resources, you might consult with the owner of the resources to determine the sensitivity of this information.
6. If you feel that these patterns should be formally reviewed, you might set up a review panel comprised of representatives from the security administration staff, the suspected user's management, and possibly the auditing staff. This review panel should meet with the user to determine the cause of the access activity.
7. If the panel decides that the cause of the activity was malicious or destructive in nature, a formal warning should be issued to the user. If your organization supports a probation program, you might also consider putting the user on probation.

   The review panel must have management backing and proper authority to enforce any agreed upon action.

   Note: At this point, you should continue to monitor the user's activity. If the excessive violation pattern continues, you should be prepared to take action against the user, possibly dismissal. Management must, of course, support this type of action.

14.3 Conclusion

Your procedure for handling violations must be tailored to your organization and to the sensitivity of the information available. You must also take into account the suspected users. Often, a user may simply be accident prone and incur excessive but unrelated violations.

You might not discourage the disgruntled employee or the dedicated internal hacker, but you will discourage the casual inquisitive employee. In addition, you will at least be prepared to take disciplinary action and enforce the security that you are taking so much time to implement. A procedure such as this one might sound severe; however, with such a procedure in place, employees become quickly aware of how seriously your organization is facing security issues.

Chapter 15. Defining Security Maintenance Procedures

Ongoing maintenance should be an important concern during and after the security implementation. This maintenance will take the form of updates to the CA-Top Secret Security File, as well as maintenance to the CA-Top Secret software itself. It is important that your maintenance procedures be in place, so that the approach is defined before receiving the first request.

If you have chosen a gradual approach to security implementation (implementing functional areas and facilities one at a time), maintenance will become a requirement before the implementation is completed. Your maintenance procedures should be designed to anticipate these requirements.

15.1 CA-Top Secret Security File Maintenance

As your environment changes, as is common in most installations, you will be required to revise your security definitions to reflect these changes. It is important to determine that the changes to security definitions are both necessary and legitimate. For this reason, you should have a CA-Top Secret Security File maintenance procedure which allows you to ensure that the requested revisions are correct and authorized.

15.1.1 Verifying Change Requests

If the organization is small, and the security administration staff can easily identify and control all users and resources, then the central administrators might be able to verify the requests for changes.

If the organization is large, it is difficult for the central staff to know all users and resources. They will have to depend on other individuals to verify change requests. In large organizations, or even in small ones, it is recommended that the representatives of the functional area that owns the resource(s) be responsible for verifying the necessity and accuracy of change requests. Requests should be made in writing with the proper authorization.

15.1.1.1 Maintenance Request Forms

Many installations design security maintenance request forms that are completed by the appropriate functional area and are approved by the appropriate functional authority. The forms are then submitted to the appropriate administrator for revision of the Security File. The forms are then filed as a permanent record of the request. These forms should contain all of the information necessary for the revision, including effective date, resource name and level of access required, user or profile name, and expiration date if the request is for temporary access. A sample request for Security File maintenance can be found in Appendix C.

15.1.1.2 Proper Maintenance

Be sure that your maintenance activity follows your original Security File design. Be careful that your profile structure is not compromised by numerous requests for update to user ACID records. Review each request to ensure that the request falls in the appropriate place in the Security File. It is possible that the requestor is unfamiliar with the structure and has requested an update for an inappropriate ACID. You might have to review the request with the requestor and modify the request before the update is actually made to the Security File.

15.1.2 Designing Procedures for Quick Turnaround

Your CA-Top Secret Security File maintenance procedure should be designed for quick response. The procedure should be designed in such a way that the requestor can receive a quick turnaround for the request. If quick response is not practical, then the turnaround time for requests should be communicated and understood by all user areas so that they can effectively plan for timely Security File revisions. Of course, emergency procedures should be available for immediate response when required.

The ability of a central security administration staff to respond quickly to maintenance requests can determine whether or not you choose to decentralize CA-Top Secret security maintenance. If certain areas require more timely response than is possible at the central level, you may choose to decentralize maintenance for those areas. Of course, if you have properly designed your Security File such that the problem areas are already divisions or departments, decentralization is simple.

15.2 System Software Maintenance

In addition to security product maintenance, maintenance procedures on other systems products which may impact the security system should be developed.

VSE Security Interface: CA-Top Secret works through the VSE Standard Security Interface and is rarely impacted by VSE maintenance. Occasionally, IBM maintenance is applied to these interfaces and a change to CA-Top Secret may be required. If you receive early releases or special releases of VSE maintenance which revise these interfaces, you should take special care in applying and testing this maintenance with CA-Top Secret. Testing procedures for operating system software changes and upgrades should always include a verification of basic security system functions as part of the plan.

You should also ensure that maintenance to interfaces of other vendor products still function properly with CA-Top Secret. Testing CA-Top Secret should always be a part of your test plans for supported vendor software.

Chapter 16. Developing Testing Procedures

As with any software—vendor or in-house developed—initial testing and testing after revision are important tasks in ensuring that the software is functioning as required. It is important to develop test plans for CA-Top Secret that you can use throughout implementation and whenever CA-Top Secret maintenance is applied. It is also a good idea to test the significant interfaces whenever vendor maintenance is applied.

It is relatively easy to test CA-Top Secret performance. The important thing to remember about CA-Top Secret is that all accesses to a particular resource are handled in the same manner; that is, to CA-Top Secret, there is no difference between data set access through batch and data set access through II (other than facility limitations). All checks are done out of the standard interfaces that are part of the VSE operating system and its access methods.

What does this mean? It means that it is necessary to check all access to resource combinations (data set access, CICS FCT access, program access etc.), but once tested in one environment, it is not necessary to check other environments that use the same resources. An exception to this would be if different environments are being run in different modes.

Typically, an effective test plan would contain:

1. Series of batch jobs accessing programs, data sets, and combinations of access characteristics that are appropriate to the controls in your organization. There should be a set of jobs that always fail, with documentation describing the expected failures in the JCL, and another series that must successfully execute.
2. For special applications (such as CICS), special application simulating procedures with attempted access to all resource types used in your organization. Again, certain functions should be set up to fail for documented reasons, and others must succeed.
3. If necessary, the aforementioned processes should be run by both normal users, administrative ACIDs, and undefined users to cover all possibilities.
4. By segregating the tests into resource types (for example, CICS versus batch), useful tests will be available to quickly and effectively evaluate specific system changes such as a new release of CICS.
5. Test results should be saved for comparison with those saved from prior tests and for comparisons with the next series of tests, in case there is any question of correct system performance.

TSSSIM Utility for Testing: TSSSIM allows you to test access authorizations for any users or resources. After you have applied CA-Top Secret maintenance, you may wish to develop test plans that use TSSSIM to verify that your resource access authorizations are still behaving as expected. Of course, you can also use TSSSIM to verify that you have defined resource access correctly whenever you update the CA-Top Secret Security File. See the *Troubleshooting Guide* for more information about TSSSIM.

Chapter 17. Customization

Although CA-Top Secret has tremendous flexibility in meeting the security requirements of most installations, your installation may face a requirement that cannot be accommodated by CA-Top Secret as delivered on the CA-Top Secret installation tape. In this situation, customization may be appropriate.

17.1 Common Reasons for Customization

Customization is most often used in the following situations:

Facility Interfaces: Standard IBM macros are often used to interface CA-Top Secret with a facility that is currently not supported by Computer Associates.

CA-Top Secret is SAF-compatible at the IBM RACF macro level. This means that CA-Top Secret will be upward compatible with interfaces that are developed using the standard IBM RACF macros.

Customization that is not based on the use of these macros or CA-Top Secret supplied interfaces may require rewriting, or may become totally unusable in subsequent releases of CA-Top Secret.

CA-Top Secret Installation Exit: Customization is used to modify CA-Top Secret behavior to meet special customer requirements through the CA-Top Secret installation exit.

The installation exit provides initiation, validation, logging, message, CA-Top Secret Security File change, and other exit points for user routines. Customization at this level has been successfully done to add features to CA-Top Secret. The exit has been used to:

- Translate messages into different languages.
- Keep multiple CA-Top Secret Security Files in synchronization across CPUs.
- Provide interfaces for second level authentication devices.
- Log additional information to SMF or to the Audit/Tracking File.

Of course, customization using the installation exit is not limited to the examples detailed. However, it is strongly recommended that the installation exit not be used to bypass security or to change CA-Top Secret behavior to behavior that does not complement documented CA-Top Secret features.

17.2 CA-Top Secret Application Interface

Customization is used to modify system or application programs to call CA-Top Secret through the CA-Top Secret Application Interface for specialized security checking. The use of the Application Interface is limited only by the time and creativity of your systems and programming staff. Use of the interface will not change CA-Top Secret behavior. It allows you to perform additional security checks for user-defined requirements.

The Application Interface has been successfully used to:

- Eliminate in-house application security systems in online systems (such as CICS).
- Provide further levels of security beyond file level protection.
- Control access to online functions within online applications.
- Control use of job class and accounting information.

17.3 Conclusion

Avoid customization through any other means than that detailed above. Computer Associates is committed only to support the CA-Top Secret capabilities—that is, the installation exit and the Application Interface—and to support interfaces through the standard IBM macros.

Many CA-Top Secret customers have successfully customized their use of CA-Top Secret through the available capabilities and macros. However, it is strongly recommended that you exercise careful analysis and planning, including research of existing CA-Top Secret capabilities, before deciding to customize. Often a reevaluation of the desired approach can eliminate a customization requirement.

Detailed information on customization for specific facilities can be found throughout the *Implementation Guides*.

Chapter 18. Conversions from Other Security Software

Many CA-Top Secret customers have successfully converted from other security software products. While no two security products can protect and control access to the same facilities and resources concurrently, CA-Top Secret can live concurrently with many of the controls used by other security products.

The objective, of course, is to replace your existing security software with CA-Top Secret while minimizing the impact on your environment and your user community. Depending on the security product currently installed, certain CA-Top Secret capabilities can be activated. Regardless of the security product in place, you can build the CA-Top Secret Security File completely without obstructing the security mechanisms of your current security software.

Although systems programming support will be necessary to de-install your existing security software, systems programming support or modifications are typically unnecessary to convert to CA-Top Secret. As suggested throughout this guide, planning and coordination among all groups is critical to a successful conversion.

The scope of this task depends on how thoroughly you have implemented your existing security product and the size and complexity of your organization. Remember that you have already built most of the foundation required for a successful security implementation. This often makes a conversion to CA-Top Secret much simpler than a full-scale security implementation.

Chapter 19. Developing Security Awareness Programs

Each implementation is unique because there are so many variables involved. But the most significant variable is that, since people are involved, security becomes an emotional and political subject. People might feel threatened by the advent of security in your organization. They might feel that it will interfere with their jobs and keep them from the resources that they need. They might also feel that their activities are now being observed.

Therefore, a security implementation is best handled as a psychological implementation as well as a technical one. The proper psychological environment for security must be created along with the technical procedures.

This environment must be planned. Support for security within the organization must be developed, courted, and encouraged if permanently successful security is an important concern of the organization. Without the active support of all involved areas, security in an installation can be at best ignored and at worst tampered with.

Security awareness programs are time-consuming because they take time to develop and because they must reach all affected employees in the organization. But the time spent is a worthwhile investment. A good security awareness program should result in acceptance and support of the security program in your organization.

19.1 Awareness Program Goals

The major goals of a security awareness program should be to:

1. Cultivate the cooperation of each affected corporate area.
2. Educate each affected individual in the use of CA-Top Secret.
3. Communicate to each individual the corporate security policy, the organization's position on security, and what is expected of the individual.

19.1.1 Cultivating Cooperation

It is more effective if every individual in your organization monitors the security program in their own area, than if the security administration area or security project team is solely responsible for this activity. You also have a better chance of a solid security implementation if the entire organization is behind it.

There are a number of functional areas involved in the use of the security product, and it is an important step to create willing users of the product. This is not as difficult as you may think, but it does take time and careful security implementation planning. The functional areas most often involved include: the systems software area, the applications area, operations, the auditors, and the applications end users. The next sections discuss each area in relation to why they may be opposed to security, why their cooperation should be cultivated, and how to cultivate that cooperation.

19.1.1.1 Systems Software Area

These individuals are probably the most technically talented and clever in the organization. Until a security product is installed, not only do they have free access to all resources, they are probably aware of more different and creative ways to access those resources than any other area in the site, and they have probably tried most of them. This is the area most likely to consider breaking or bypassing the security system a challenge.

By the nature of their jobs, they require powerful access to systems resources. They do not, however, normally require direct access to applications resources, except for DASD management functions. They are often opposed to the security system because they fear that it will get in the way of doing their job.

Cooperation should be cultivated in this area for two important reasons. First of all, CA-Top Secret maintenance will probably be the responsibility of this area. To effect smooth maintenance procedures, a cooperative spirit should exist between the software area and the security administration area. Secondly, the systems software group often uses facilities capable of bypassing security. It is important to restrict the use of these facilities and to gain this group's cooperation in doing so.

Gaining Support: Security should be implemented for this area and for any area so that protection is provided without limiting the function required to handle the job. You can gain support by implementing security in this area in such a way that:

- System resources are protected, and only authorized ACIDs are allowed to access them at specific access levels for required functions such as VSE maintenance or VSE subsystem maintenance. It is important to note that these resources will no longer be available to anyone other than the system software area. They should continue to be available within the software area, but only at the needed access level, so that system resources are not accidentally damaged.
- Administrative ACIDs are available that will give the system software area the authority to handle all required functions against non-system resources, such as DASD maintenance.

As long as the system software person is not continually working at cross-purposes with CA-Top Secret while trying to do his job, he will come to view the security product as a support feature rather than an inhibitor. This, of course, requires careful security design and implementation in this area.

19.1.1.2 Applications Area

These individuals are involved with developing the business software required within the corporate environment. As part of their function, they are required to access only those resources making up their application and some globally accessible system resources. Initially, there may be a fear of CA-Top Secret.

Actually, these areas may welcome CA-Top Secret if they are properly educated in its use. CA-Top Secret provides an applications interface that allows the applications areas to use the security system to provide additional application security needs. This gives the applications area a tool to simplify design wherever additional security is required. This also gives the security administration area the opportunity to eliminate the homegrown application security systems and to centralize all security requirements, as well as to standardize security administration.

Each application will require different security definitions, so protecting this area may be a slow process. Each application design should be evaluated for effective protection. The security administrator is well advised to involve the affected application area in the security definition process.

19.1.1.3 Operations

The operations staff has a very important but harrowing task to perform. They have to get production processing completed on time while contending with problems such as system unavailability, hardware problems, production abends, CPU utilization, and now CA-Top Secret. You can understand how the operations area can easily view security as just another headache that can get in the way of completing production. But you must take the time to cultivate the cooperation of the operations area in supporting CA-Top Secret, or they may try to undermine it.

Production security must be carefully designed and tested to avoid security abends. If security abends occur, the operations area must have procedures available that will allow them to get production through with minimal delay.

Although the operations staff usually is the least involved with CA-Top Secret, they can be the most seriously impacted by it. Careful consideration should be made to ensure that production will run with the proper protection but without being impacted by the security implementation.

If careful consideration is given to the needs of this critical area, the operations staff can come to realize that CA-Top Secret is protecting the resources for which they are responsible, and they may come to depend on it.

19.1.1.4 The Auditors

The auditing area is probably the only area that enthusiastically supports the CA-Top Secret implementation, since it is the auditors' responsibility, in most environments, to ensure that corporate resources are properly protected and to point out where these resources are exposed to unauthorized review, modification, or destruction. The auditors do not need much convincing that a security product is required in your environment.

You can, however, take additional steps to enlist their support in the security implementation. In fact, if you include them in the implementation process, they will not be in a position to criticize and force rework of strategies at a later time, because their direct input will be used in designing security measures for the environment.

Procedures for Auditors: In addition to requesting their input on the security design, you can also set up procedures for the auditing staff which allow them to take advantage of the auditing features provided in CA-Top Secret. These procedures should be developed early in the security design phase to allow the auditors to monitor activity as the implementation progresses. Auditors may be able to offer input on design requirements as a result of this review, and their input could prove significant in tightening the security procedures developed.

19.1.1.5 Applications End Users

This group is probably the least knowledgeable in data processing, but the most dependent on the facilities provided by the applications and systems areas to perform their specific job function. They are probably the most knowledgeable, however, in how the resources used in their areas should be accessed, and by whom. They are also a good source in determining what information is critical to the organization, and potential abuse of this information. For these reasons they require special handling.

The end user's understanding of the nature of the security software is generally limited to the idea that it is being implemented to prohibit external attack on corporate resources, and that it should be invisible internally. In fact, their greatest exposure to the need for security probably comes from inaccurate attempts by television and the movies to portray wide-open computer access. Needless to say, they are very surprised when they inadvertently interface with CA-Top Secret for the first time.

The end users will support the use of security, but not if it becomes something that prevents them from simply doing their job. Therefore, security for this group should be defined so that it is as transparent as possible.

Provide a Central Area for Administration: Another security concern for end-users, particularly if they must deal with an application that has internal security requirements, is confusion as to where they should go to handle a security problem or to set up a new employee for computer access. This makes it advisable to consolidate all security services into a central area, from the users' point of view, even if that area is actually a decentralized security area. Encouraging applications development areas to abandon homegrown security in favor of taking advantage of the CA-Top Secret Applications Interface will simplify this security centralization effort.

If you take the time to ensure that you have considered the psychological needs of each area, as well as the technical requirements, your implementation will proceed more smoothly than you might expect. In fact, you may find that you will be receiving assistance and support from all of these areas. This is an important step toward achieving truly effective security in your environment. Someone once said that, "...people fear that which they do not know." An important task of the security awareness program is to develop educational procedures so that each area is aware of CA-Top Secret, how it functions, what is expected of them, and what the product can do for them. These procedures do not necessarily stop with the initial implementation, but should be designed to provide information to the users concerning new security features and facilities. Also, education should be made available when new users come into your organization.

19.1.2 Subject Matter

Some of the subjects that should be addressed and the intended audiences are discussed next.

For Systems Software Personnel: CA-Top Secret installation and information on how CA-Top Secret interfaces with the operating system.

For Systems Software and Application Development Personnel: Information on how CA-Top Secret can be used to assist in the design of new or existing system and application facilities through the CA-Top Secret Application Interface.

For the Auditors or Any Auditing Area: Information on how to use CA-Top Secret to monitor the data processing environment without impacting the operation of the site.

For All Users: Information on ACID and password requirements, including:

1. How often the password should be changed, and the procedure for revising it.
2. Under what circumstances an ACID can be suspended, and what to do about it.
3. What kind of violation messages they may encounter, and what action is required for each.
4. The nature of the CA-Top Secret Last Used Message and instructions on how to verify that the last use of their ACID was legitimate.

19.1.3 Developing Training

Individual training programs can be developed for each functional area, or training can be organized by subject. The training should be repeatable so that it can be presented to new users at regular intervals.

The most significant point to be made as part of the education process is that security does not hurt and can in many cases improve the effective use of data processing resources in your organization.

19.2 Communicating the Security Policy

For the security policy, or document of security objectives, to be understood and accepted within the organization, it must be effectively communicated to all users. It is recommended that you use a combination of the following methods of communication:

Global Distribution Distribute the physical document to all users. The document could be included with your organization's personnel policies and procedures manual.

Formal Presentations Formally present the security objectives to all users. This could be included with CA-Top Secret training.

Performance Review Include adherence to security policy in the job performance review checklist.

You must make clear to each user the position the organization takes on security issues and the responsibilities of each user toward the security program.

Security Seminars: Many organizations develop security awareness seminars where they present the necessity for security, what the organization is doing about security, and what the user is expected to do about security. These seminars are usually quite effective in communicating the corporate attitude toward security.

Security Films: There are a number of good security awareness films available for purchase or rental for security seminars. You can contact your CA-Top Secret user groups or security organizations for information on these films.

Chapter 20. Scheduling Ongoing Evaluation

Even after your CA-Top Secret security implementation has been completed, you should not stop monitoring and evaluating the effectiveness of the implementation. Your environment will change, and your implementation of CA-Top Secret must be as dynamic as your environment.

20.1 Evaluation Team

You might establish a security evaluation team—even during the implementation—which might be comprised of the members of the initial project team. Minimally, the team should include: the security administration area, the auditing group, the systems software area, the applications area, operations, and possibly end user representation.

Team Responsibilities: This team should obtain and evaluate feedback from each corporate area affected by the security implementation. The results of this evaluation may suggest revisions to the implementation plan. If the implementation is completed, the results may suggest revisions in security direction or design to meet a changing environment. The results may even suggest revisions to the security policy or document of security objectives.

Remember that security considerations should become a part of any environmental change once your organization is committed to implementing a security product. These considerations should become part of the evaluation or modification checklist for each proposed acquisition or modification in your environment. Otherwise, you may find that new or revised software has security exposures after your organization is committed to the change.

20.2 Annual Security Review

Although you should be continually monitoring your security environment, it is recommended that you plan an annual security review by qualified professionals.

Appendix A. Sample Security Files

This appendix contains examples of:

- A Corporate Level Policy (First Tennessee Bank, written by Bob Wicksel)
- An Application Level Policy (Human Resource Security Policy)

A.1 Corporate Security Policy

All computer-based data and programs are corporate assets and, as such, must be protected against unauthorized access, disclosure, and/or manipulation.

The Transaction and Information Group under the direction of the Priority Committee, as part of its custodial responsibility for the main computer data and programs, will assure that certain base security controls are defined, implemented, and administered for these corporate assets. The Transaction and Information Group also has responsibility for advising the user/owner of those additional controls that can be added to provide further security beyond the base controls. The user/owner of the respective application data and programs will assume the responsibility for determining which of these additional control features will be employed within their respective functional area and for assuring that the proper ongoing administrative procedures are observed.

A.1.1 Base Security Controls

Base security controls for the First Tennessee host computer environment are established by the security task force. These controls are monitored and administered via the CA-Top Secret security software package.

The implementation of base security controls, with the framework of CA-Top Secret, will be based upon the principle of "least possible privilege". Under this principle, initial communication with the host computer, access to data/programs and the use of computing functions will be summarily denied unless specific authorization has been granted and is resident within the CA-Top Secret Security File.

Base controls 1 through 3 deal with the initiation of communication between the user and the host computer; three control levels, access, identification, and authentication must be satisfied to establish this base linkage.

Base controls 4 and 5 determine the information resources (data/programs) and computing functions the user will have access to.

Base control 6 deals with the mandatory changing of user passwords at a regular, specified interval.

Base control 7 addresses the logging and reporting of security violations.

A.1.1.1 Device Access Control

All computer terminals and card readers must have a unique, fixed hardware identification code known to the security system to communicate with the host computer. The Transaction and Information Group will assign this code to all existing devices, and, for any such devices added to the system. Attempts to gain access by any unknown device will be denied.

A.1.1.2 User Identification Control

All authorized users must have a unique personal identification code. This code must be supplied immediately after the initial host communication link is established, or further access will be denied and the communication link will be terminated. The Transaction and Information Group will assign this code based upon appropriate authorization supplied by a recognized user/owner.

A.1.1.3 User Authentication Control

All authorized users must have a unique personal password that is associated with their personal identification code. This password must be supplied immediately after their identification is successfully validated, or further access will be denied and the communication link will be terminated. Each user is responsible for the selection and protection of their personal password.

A.1.1.4 Information Access Control

All corporate information resources are owned and are identified by owner within the security system. Information resource owners must authorize access rights for each user requiring access to those resources. Access control will be automatically enforced by the security system. Attempted unauthorized access to owned resources will be denied.

A.1.1.5 Computing Function Control

All host computing functions (for example, the insertion, changing, or deletion of data; the execution of computer programs; the creation, copying, or deletion of data files/programs) will be protected by the security system. Resource owners must authorize computing function capability for each user with these requirements. Attempted unauthorized performance of computing functions will be denied.

A.1.1.6 Mandatory Changing of Passwords Control

Each authorized user must change his/her personal password every thirty (30) days. The security system provides this capability directly to the user, therefore the responsibility for password security rests with each user. Passwords may be changed more often as necessary, but non-observance of the 30 day requirement will result in the automatic suspension of access rights.

A.1.1.7 Violation Logging and Reporting Control

All security violations, whether intentional or unintentional, will be logged when they occur. Security violation reports will be prepared and distributed to appropriate individuals, such as the security office, EDP Audit, owner department manager, and so on.

Repeated intentional security violations by individuals may result in suspension of computer access rights, disciplinary action, and/or termination.

A.1.2 Recommended Additional Owner Controls

In addition to the base security controls, it is strongly recommended that all information resources (data, programs, and so on) owners carefully evaluate the additional controls listed in this section and, based upon the potential risk and/or exposure, select those appropriate for their application.

The combination of base controls and the following additional controls provides the user/owner with a comprehensive set from which to build an effective, yet tailored, security program.

A.1.2.1 User Device Restriction Control

This control ties the unique personal identification code to specifically identified devices (terminals). Attempts to gain access from an unauthorized device would be denied.

A.1.2.2 User Facility Restriction Control

This control is tied to personal identification codes, and may be used to limit user access to only specified computer facilities (hardware/software access mechanisms), such as CICS or batch. Attempts to gain access to unauthorized facilities will be denied.

A.1.2.3 Unattended Terminal Locking Control

This control provides each user with the ability to lock their terminal, preventing unauthorized access, in the event the terminal is left unattended for a period of time. Attempts to gain access from a locked terminal will be denied.

Note: This control is recommended in place of an automatic time-out feature which could cause loss of data or dysfunction within a particular application.

A.1.2.4 Day(s) of Week Restriction Control

This control provides for the limiting of individual access privileges for specific users to specified days of the week, (for example, Monday through Friday, Wednesday only, and so on). Attempts to gain access on restricted days will be denied.

A.1.2.5 Time of Day Restriction Control

This control provides for the limiting of individual access privileges for specific users to specified hours of the day (for example, 8:00-5:00, 4:00-12:00, and so on). Attempts to gain access during restricted hours will be denied.

A.1.3 Central Security Administrator - Responsibilities

This section describes the functional responsibilities of the central security administrator (CSA) at First Tennessee Bank. The mission of the CSA is to administer a corporate-wide data security program designed to protect against unauthorized access, the intentional or unintentional disclosure, manipulation, and/or destruction of computer-based corporate information assets.

The objective of the First Tennessee data security program is to minimize potential exposure of the corporation. The approach to meeting this objective is based upon the following actions:

1. Document existing security controls for all computer-based applications.
2. Evaluate existing security controls, in terms of strengths and weaknesses, to estimate current risk/exposure levels.
3. Install standardized base controls, to be applied to all computer terminals in the corporation. For example:
    a. Assign each computer terminal a unique identification code to be automatically verified upon each computer access attempt.
    b. Assign each authorized person a unique identification code to be automatically verified upon each computer access attempt.
    c. Assign each authorized person a unique, secret password to be automatically verified upon each computer access attempt.
    d. Restrict access, disclosure, manipulation, and erasure capabilities to only authorized individuals for each computer-based application.
    e. Restrict the ability to initiate computer programs, copy computer data files, and perform other computing functions to only authorized individuals for each computer-based application.
    f. Install automated mechanism to log and report all data security violations.
4. Develop recommended additional security controls to further enhance the security level within a particular functional area:

a. Automatically enforce mandatory changing of secret individual passwords at specified intervals.

b. Automatically enforce restriction of individual users to only specified computer terminals.

c. Automatically disconnect unattended, inactive terminals after specified time limit expiration.

d. Automatically enforce restriction of individual access to specified days of the week only (Monday-Friday, and so on).

e. Automatically enforce restriction of individual access to specified time of day only (8-5, and so on).

f. Automatically control each individual's ability to display, manipulate, and/or erase only authorized data files, programs, and so on.

g. Automatically control each individual's ability to initiate computer programs, copy computer data files, and perform other computing functions based upon granted authority.

5. Specific CSA administrative functions:

a. Develop and install a comprehensive data security violation monitoring capability.

b. Perform regular reviews of all security violation reports and initiate appropriate corrective actions.

c. Regularly distribute security violation reports to business unit and, as required, department management for follow-up action.

d. Develop a corporate security awareness program to inform and educate all FTB employees of their security responsibilities.

e. Assist department security coordinators in the communication and resolution of highly technical security issues to other departments (T & IS).

f. Install automatic enforcement mechanisms to enforce and maintain base controls.

g. Develop and recommend additional data security controls to department security coordinators.

h. Maintain comprehensive documentation of the corporate security environment.

The CSA function will reside in the Transaction and Systems Information business unit, but will be accountable to all appropriate corporate management charged with data security responsibility. Further, the activities of the CSA will be closely monitored at all times by the EDP Audit group.

A.1.4 Departmental Security Coordinator - Responsibilities

Each business unit within the First Tennessee corporation is responsible for the naming of one or more department security coordinator(s) to provide first-level security administration for the major functional departments within that business unit.

This section describes the functional responsibilities of the Department Security Coordinator (DSC) at First Tennessee Bank. The DSC role is performed at the department level; all the functions and responsibilities defined here relate to that level.

The mission of the DSC is to assist the Central Security Administrator in the implementation and ongoing maintenance of the corporate data security program.

The DSC will be the focal point for all security-related communications from a department to the Central Security Administrator.

Specific DSC Administrative Function:

1. To document the existing computer application requirements for his/her department, as follows.
   a. Prepare a complete list of all computer terminals used in your department, including their location.
   b. Prepare a complete list of all current user IDs, including the user's name, phone number, location (mail code), computer applications used, and primary functions performed.
   c. Prepare a complete list of all computer files used by your department.
   d. Prepare a complete list of all computer programs used by your department.
   e. Prepare a complete list of any current password protected computer files used by your department.
   f. Prepare a cross reference matrix that relates each individual user to the previously mentioned items, including required read, write, update, scratch, and create authority of computer files for each.
2. To validate the implementation of the base controls.
3. To select, install, and perform administrative functions for all recommended additional data security controls.
4. To regularly receive and review security violation reports and take appropriate actions.
5. To report security violations to department management for follow-up action.

A.1.5 Introduction to CA-Top Secret

Data security is a key issue with the First Tennessee National Corporation. Computer information resources, whether in the form of programs or data, are viewed as corporate assets and therefore must be protected from either intentional, or more commonly unintentional, destruction and/or misuse.

CA-Top Secret was selected by First Tennessee over IBM's RACF and CA-ACF2 because of ease of installation and low overhead requirements. CA-Top Secret places no hooks into the operating system and is therefore independent of normal system maintenance. It does, however, utilize the standard IBM RACF interface for inter-system communications.

Although the implementation of this package will necessitate many changes in our current environment, and the related procedures, every effort will be made to minimize disruption and loss of productivity.

A.1.6 Impact Areas

The implementation of CA-Top Secret security will require both short and long term changes to our current operating environment.

In the short run, the immediate changes affecting current day-to-day activities are:

1. Limited, or restricted, access to previously available data and libraries.
2. Production problem resolution must now be coordinated with, and authorized by, production (3rd floor C/T) management.
3. Previously unenforceable standards will now be enforced.

The longer term changes will include:

1. Major changes to existing library control function.
2. Formalized procedures for data access authority.
3. Enhancement to existing standards and addition of comprehensive standards.
4. Data security reviews of new or modified applications.
5. Data security reviews of new or modified hardware.

These changes will take time, but the potential benefits are substantial in terms of both asset protection and greater productivity due to a more standardized environment.

A.1.7 Potential Problem Areas

The following paragraphs describe potential problems that you may encounter and recommended solutions to those problems.

A.1.7.1 Mandatory Changing of Password

Under CA-Top Secret, you are totally in control of, and responsible for, your secret password. Your II password is no longer operative and has been replaced by your CA-Top Secret password.

In terms of responsibility, you have already read how CA-Top Secret discourages you from entering your password at logon (except in nondisplay mode). In keeping with this philosophy, you will be required to change your secret password at least every 30 days. You may change it more often, as necessary.

Three days prior to your password's expiration you will begin receiving a CA-Top Secret message informing you that your password will expire within three days. For your convenience, it is recommended that you change your password as soon as you get this message, at the next logon.

CA-Top Secret will not automatically suspend your ID unless you totally ignore this message. That is, if you do not use your ID for 45 days, it will not be suspended, but you must change your password the first time you logon.

1. To change your password, at logon (password prompt)

   ```
   =>  ENTER:  OLDPASSWORD/NEWPASSWORD
   ```

2. You will receive the message PASSWORD CHANGED.

Keep in mind that:

- Your password must be at least four characters long.
- You cannot reuse any of your last three previous passwords.

Every time you log on you will get a last used message displayed on your terminal. This message informs you of the date, time, facility used, system used, and a numeric count of the number of times your ID has been used. If you suspect, or are sure, that your ID is being used by another individual you should change your password immediately.

Remember:

- Do not share your password with other individuals.
- Do not write your password down and leave it where it can be obtained by others.
- Change your password regularly.

A.1.7.2 Use of Production High Level Indexes

The access rules are primarily determined based upon the current high level indexes in use. That is, production files (data sets) are generally protected from all access except for production batch processing and authorized terminal inquiry/update functions. Systems development users have been authorized read access, by group, to the applications they are responsible for.

CA-Top Secret enforces the DPS standards that have been defined to it. Therefore, make every effort to conform to the current published standards. Whenever possible use the TEST prefix to eliminate conflict with production indexes.

Due to the previous inability to enforce standards, many users have created test mechanisms that either bypassed or ignored the published standards. Without exception CA-Top Secret will intercept each and every one of these and prevent them from accomplishing the desired result.

All test jobs and/or libraries that you currently use should be reviewed to ensure compliance with this rule. A thorough review of your existing procedures, rather than job-by-job experimentation, will save you lost time and headaches.

Exceptions to this rule must be justified and will be addressed on a case-by-case basis.

A.1.7.3 Access Change Rules

There are many situations that will require changes to the currently defined access rules such as:

- employee new hire, transfer, or termination
- major system conversion/parallel
- special project requirements
- vendor imposed exception conditions
- production problem resolution

Requests for access rule changes will be subject to base control standards established for all T & I users:

- unauthorized access to production data is prohibited.
- unauthorized access to production libraries is prohibited.

All requests for access rule changes are to be made in the following manner:

- Document the requirements and current restrictions.
- Obtain approval from your designated Departmental Security Coordinator.
- Forward approved request to the Central Security Administrator, in advance of need date.

The above documentation may be submitted by memo, and countersigned by the DSC (Departmental Security Coordinator).

Additional information may be required—such as the access duration, specific user IDs affected, and so on. Please try to be prepared to answer these questions.

A.1.7.4 Production Problem Resolution

The function of production problem resolution will be strictly monitored to ensure adherence to the security standards. In the past, many types of problems could be resolved informally by knowledgeable personnel. This will no longer be the case. The access restrictions placed upon T & I personnel will require a formalized procedure to be initiated to obtain the needed access to resolve most production problems.

The procedure to be followed for the resolution of production problems is:

1. A properly documented I/R form is required for each problem.
2. The I/R must be presented to the acting central production manager (or designee, if not present) for his/her review.
3. The central production manager, or designee, is authorized to grant the use of special IDs that have appropriate access capabilities needed to resolve production problems.

   Note: All use of these IDs will be monitored and must be accounted for with supporting problem documentation.
4. The central production manager, or designee, will record the assigned special ID number on the I/R and ensure that the problem resolver's name is also recorded on the document. The password for the ID will be given to the problem resolver.
5. The problem resolver will use the ID provided to fix the problem. Upon satisfactory resolution, he/she will return I/R, with completed resolution data, to the central production manager or designee.
6. The central production manager will deactivate the ID by changing the password and recording the password in a secure location.
7. The central production manager will route a copy of the completed I/R to the Central Security Administrator for reconciliation to the audit trail report.

A.2 Human Resource Security Policy

Subject:	Human Resource Security Policy
Effective:	For All Divisions on July 1, 1990
Objective:	To ensure that human resource information is protected from accidental or intentional unauthorized modification, destruction, or disclosure.
Issuing Officer(s):	Vice President - Personnel
Contact(s):	Vice President - Personnel/Operations Vice President - Administrative Planning Vice President - Internal Audit Vice President & Treasurer - Financial Control
Cross Reference(s):	None

A.2.1 Purpose

Our purpose in establishing a data security policy is to ensure that human resource information is protected from accidental or intentional unauthorized modification, destruction, or disclosure. Further, due to the sensitive and confidential nature of this information, it is critical that access to it be highly restricted.

A.2.2 Policy

Our Human Resources Security Policy defines the information to which the policy applies, who has proprietary rights to the information, individual accountability, responsibility for procedures, and outlines specific responsiblities within the organization.

A.2.2.1 Scope

This policy applies to all human resource information created or maintained within the corporation and its subsidiaries. Information includes data recorded on physical documents and on automated devices. The policy also applies to automated procedures and facilities (source code, job control, load modules), because these are the means through which the data can be accessed, altered, or destroyed.

A.2.2.2 Proprietary Rights

Human resource information is the property of the Profit Center responsible for the data.

The corporate personnel/payroll function is the custodian of the data and will centrally process all maintenance to human resource data.

For all Profit Centers except Central Office: The authority to grant access to the data resides in the personnel function within the appropriate Profit Center. Requests for access to the data must be channeled through the corporation personnel function only with the approval of the appropriate Profit Center personnel representative.

For Central Office: Central Office is the repository of the data and is thus ultimately responsible for its protection. The corporate personnel/payroll function has complete access to data for all Profit Centers without the approval of the Profit Center personnel function, because they are responsible for corporate-wide processing of the data. Only the corporate personnel/payroll function may fully access production information. Each Profit Center may access its own production information.

None of the foregoing shall preclude Internal Audit from having access to the data needed to fulfill their responsibilities as detailed next.

A.2.2.3 Accountability

Any individual who is involved in unauthorized disclosure of human resource information, procedures, or facilities used to extract information is subject to punitive action or dismissal.

A.2.2.4 Procedure

Each functional unit named within this policy will maintain comprehensive procedures to support the Human Resource Security Policy.

A.2.2.5 Responsibilities

The corporation, in its role as an employer of people, has a legal responsibility as well as a moral obligation to strictly limit access to human resource information. Specific responsibilities with regard to human resource security within the corporate organizations are detailed below.

1. Human Resource Security Committee
   - To approve any amendments to the Human Resource Security Policy.
   - To review all human resource procedures developed to support the Human Resource Security Policy. It is understood that the scope of this committee relates only to human resource security matters and not to other areas which are the responsibility of the other involved departments.
   - To meet at regular intervals to review all aspects of the Human Resource Security Policy and its associated procedures.
2. Personnel
   - To validate and process approved modifications to employee personnel information in a secure manner.
   - To process and distribute reports and other personnel information in a secured manner to appropriate field personnel or other approved recipients.

- To recommend security policies governing the nature and format of employee records of the Profit Centers.
- To monitor and audit the performance of the Profit Centers in the administration of approved security policies, plans and practices.
- To monitor and coordinate the Profit Centers' compliance with employee-related legal requirements and to act as liaison with the corporation's Legal Department.
- To secure the Personnel area to maintain the confidentiality of all employee information under their control.
- To approve requested modifications to human resource procedures and facilities which are under their control and to ensure that these modifications comply with human resource security provisions.

3. Payroll
   - To process the payroll for all approved corporate organizations in a secure manner.
   - To validate and process approved modifications to employee payroll information in a secure manner.
   - To distribute checks, reports, and other payroll information in a secured manner to appropriate field personnel or other approved recipients.
   - To secure the Payroll area to maintain the confidentiality of all employee information under their control.
   - To approve requested modifications to human resource procedures and facilities which are under their control and to ensure that these modifications comply with human resource security provisions.
4. Benefit Plans Accounting
   - To process the employee savings plan system for all approved corporate organizations in a secure manner.
   - To validate and process approved modifications to employee savings plan information in a secure manner.
   - To distribute reports and other savings plan information in a secured manner to appropriate field personnel or other approved recipients.
   - To secure the Benefit Plans Accounting area to maintain the confidentiality of all employee information under their control.
5. Profit Center Personnel Function
   - To ensure that any request for extraction of human resource information is granted on a "need to know" basis. Access is only granted to data which an individual requires to perform an authorized function. It is understood that no Profit Center may have access to the human resource information of any other Profit Center, unless a reporting relationship exists.
   - To maintain a security policy for the protection of human resource information that is consistent with the Human Resource Security Policy.

6. Financial Systems

   - To ensure that any request made to Financial Systems for extraction of human resource information has been made through approved channels.
   - To secure any Financial Systems area allowing access to human resource information or documentation.
   - To approve requested modifications to human resource procedures and facilities which are under their control and to ensure that these modifications comply with human resource security provisions.

7. Internal Audit

   Internal Audit has complete access to human resource information consistent with overall audit responsibilities. These responsibilities as they relate to human resource security include:

   - To serve in a review and advisory capacity with respect to human resource security measures to ensure compliance with responsibilities as defined by the policy.
   - To review individual Profit Center security policies for adequacy and adherence.
   - To review requested accesses to human resource information on a periodic basis for adherence to this policy.
   - To perform any audit involving human resource information in a responsible and secure manner. Internal Audit will be accountable for any information gained during the course of an audit.
   - To secure any Internal Audit area allowing access to human resource information or documentation.

8. Human Resource Systems

   - To maintain the automated procedures and facilities capable of accessing human resource information which comprise the human resource application in a secure manner.
   - To ensure that access to automated facilities capable of accessing automated human resource information is restricted to members of Data Center Human Resource Systems, approved user personnel, and approved Data Center Operations personnel.
   - To implement only approved modifications to human resource procedures and facilities.
   - To secure the Data Center Human Resource Systems area to restrict access to automated procedures and facilities.

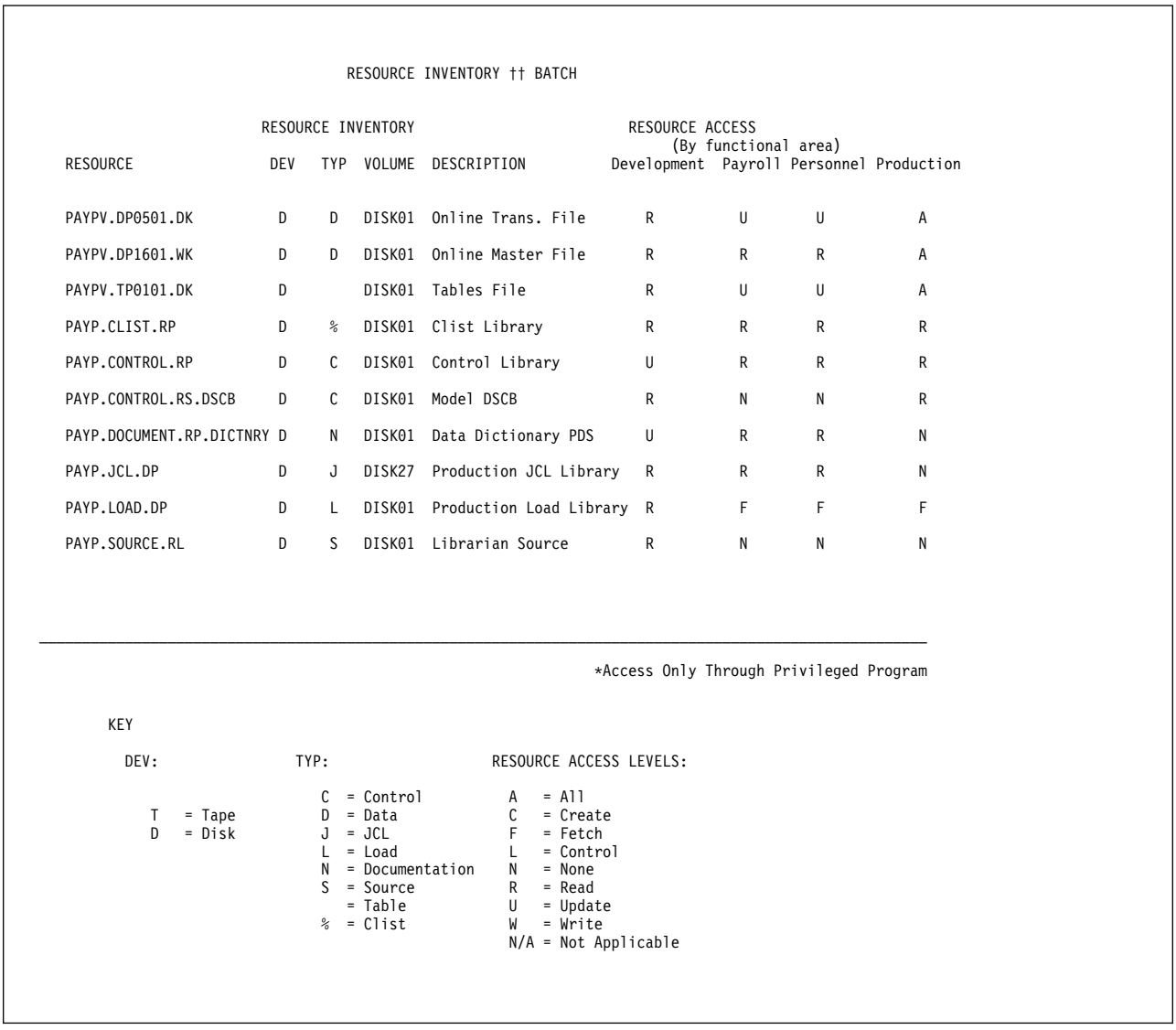
9. Data Center-Operations

   - To execute all human resource automated processing in a secure manner by authorized Data Center-Operations personnel only as requested by authorized user personnel.
   - To ensure that the distribution of human resource systems output is made only to authorized personnel.
   - To secure specified areas of Data Center-Operations to maintain confidentiality of human resource information while it is under their control.

10. Data Center-Technical Services

    - To ensure that any access to human resource information, procedures or facilities as required by the nature of their responsibilities be done in a secure and responsible manner.
    - To ensure that the security system software is maintained in a secure manner since this software is the basis for protection of automated human resource information, procedures and facilities.

Appendix B. Sample Inventory Forms



RESOURCE INVENTORY †† BATCH

RESOURCE	RESOURCE INVENTORY DEV	TYP	VOLUME	DESCRIPTION	RESOURCE ACCESS (By functional area) Development	Payroll	Personnel	Production
PAYPV.DP0501.DK	D	D	DISK01	Online Trans. File	R	U	U	A
PAYPV.DP1601.WK	D	D	DISK01	Online Master File	R	R	R	A
PAYPV.TP0101.DK	D		DISK01	Tables File	R	U	U	A
PAYP.CLIST.RP	D	%	DISK01	Clist Library	R	R	R	R
PAYP.CONTROL.RP	D	C	DISK01	Control Library	U	R	R	R
PAYP.CONTROL.RS.DSCB	D	C	DISK01	Model DSCB	R	N	N	R
PAYP.DOCUMENT.RP.DICTNRY	D	N	DISK01	Data Dictionary PDS	U	R	R	N
PAYP.JCL.DP	D	J	DISK27	Production JCL Library	R	R	R	N
PAYP.LOAD.DP	D	L	DISK01	Production Load Library	R	F	F	F
PAYP.SOURCE.RL	D	S	DISK01	Librarian Source	R	N	N	N

*Access Only Through Privileged Program

KEY

DEV:
- T = Tape
- D = Disk

TYP:
- C = Control
- D = Data
- J = JCL
- L = Load
- N = Documentation
- S = Source
- = Table
- % = Clist

RESOURCE ACCESS LEVELS:
- A = All
- C = Create
- F = Fetch
- L = Control
- N = None
- R = Read
- U = Update
- W = Write
- N/A = Not Applicable

RESOURCE INVENTORY †† CICS PRODUCTION

	RESOURCE INVENTORY			RESOURCE ACCESS		
RESOURCE	RESOURCE	TYP	DESCRIPTION	Development	Payroll	Personnel
PAYPV.DP0501.DK	PAYD	D	Transient Data	N	A	A
PAYPV.DP1601.WK	PAYTERM	F	Transient Security File	N	R	R
PAYPV.TP0101.DK	PAY1	T	Initial Transaction	N	Y	Y
PAYP.CLIST.RP	PAY210	F	Online Transaction File	N	U	U
PAYP.CONTROL.RP	PAPY320	F	Online Master File	N	R	R
PAYP.CONTROL.RS.DSCB	PAY(PREFIX)	P	Application Modules	R	N	N

KEY

TYP:

- T = Transaction
- F = File (FCT)
- P = Program
- D = Destid
- J = Journal (JCT)
- X = Temp Stor

RESOURCE ACCESS LEVELS:

- A = All
- U = Update
- R = Read
- W = Write
- B = Browse
- D = Delete
- N = None
- Y = Authorized
- N/A = Not Applicable

Appendix C. Sample Maintenance Form

A sample maintenance form is shown on the next page.

SECURITY ADMINISTRATION ACCESS AUTHORIZATION

DATE:	PAGE:
MM DD YY	OF

USER TO BE AUTHORIZED:________________

TYPE OF REQUEST:
[ ] ASSIGN OWNERSHIP
[ ] GRANT ACCESS
[ ] REVOKE ACCESS
[ ] TRANSFER OWNERSHIP TO ____________

RESOURCE ACCESS REQUIREMENTS

RES TYPE	RESOURCE NAME	ACCESS LEVELS	EXPIRY MMDDYY	TIMES OF DAY	DAYS	FACILITY	SPECIAL ACCESS THRU	
							PRIVPGM	LIBRARY

SPECIAL REQUIREMENTS & CONSIDERATIONS

SECURITY USE ONLY

	IMPLEMENTED BY: DATE:

	AUTHORIZED BY:	DEPT:	SIGNATURE:	TEL/EXT:	DATE:
AUTHORIZATION AUTHORIZATION AUTHORIZATION					

Appendix D. Developing a User Guide

Security is a global concern. It effects not only corporate personnel assigned to administer and audit security, but also end users at every level. To ensure that your security policies and procedures remain sound, it is important that all users realize that security is a team effort and that each individual plays an important role.

The best possible way to motivate the "team" is to provide each individual with knowledge of company security policies and procedures, a brief overview of the security product, and an understanding of their unique security role. How is it possible to do this in an inexpensive, organized fashion? Simple—by creating a security handbook or user guide.

This chapter is a comprehensive look at what users need to know about their company's security. It is targeted at the security administrator who is assigned the task of developing a company user guide. The material presented in the remainder of this guide should be used as a base from which information applicable to your site/users is drawn. A sample user guide can be found in the section "Sample User Guide".

D.1 User Guide Content

D.1.1 Format Considerations

Before you begin writing your company's user guide, remember that the purpose of the guide is to supply your users with pertinent security information. You want them to read it and to reference it when necessary. To be effective, the user guide should be as clear and concise as possible.

D.1.2 Glossary

One of the purposes of a user guide is to provide the user with a smooth transition into a secured environment. You should include a glossary of security-related terms. These terms help familiarize the user with CA-Top Secret which, in turn, will enhance user/administrator communication concerning security events or problem notification.

Along with CA-Top Secret terms, you should include other security terms that are commonly used at your site. For example: access, ACID, error message, facility, MODE, logon, ownership, password, permission, profile, resource, security administrator, violation, and so on. These terms are defined in the section "Sample User Guide" later in this appendix.

D.1.3 Security Policy

Your company's security policy may be a manual in itself. Although it is not suggested that the entire policy be reproduced in a user guide, it can be beneficial to include topics that are pertinent to the user. For example:

- Scope of authority—which resources are protected (e.g., data, facilities, hardware, etc.)
- Ownership—who owns protected resources
- Resource access—what are the requirements for accessing resources and whom to contact for authorization
- Resource integrity—who is responsible for ensuring that resources are being accessed, used, or modified in a secure manner
- Violations—how violations are logged and reported and action to be taken when security is breached
- Accountability—what the user is responsible for reporting
- Problem determination—who to see for help

Note: A sample security policy is supplied in the *Planning Guide.*

Resource Naming Convention Standards: When resource naming conventions are being developed or existing naming conventions are enforced, CA-Top Secret will not allow users to create resources that do not follow the standards. The user guide should clearly communicate your company's conventions or refer the user to the proper document that lists them.

D.1.4 Security Structure

In an effort to familiarize the user with the new security environment, it is suggested that you provide him with information about the company's security structure. The guide should contain a chart showing the hierarchical structure of the security environment. The chart should illustrate the user's position within the structure and identify the security administrator to whom the user should direct questions, requests, problems, and violations.

Along with knowing his position in the security structure, the user should be advised of his security responsibilities. All users must be aware that they are under obligation to protect corporate data processing assets. The following items represent some general user responsibilities:

- To keep all accounts used to access data processing resources and facilities confidential.
- To revise the passwords of these accounts at regular intervals.
- To notify the appropriate person(s) if abuse of the account is suspected.
- To actively support all security procedures.

D.1.5 Signon/Signoff Procedures

Because signon/signoff procedures are site dependent, each organization must provide their user community with both the operating system requirements as well as the CA-Top Secret requirements for signon/signoff procedures.

The procedures should serve as step-by-step instructions including all system responses such as the CA-Top Secret "Last-Used" and "Status" messages (see the section "CA-Top Secret Messages").

New User Signon Procedure: For a new user to signon to the operating system the security administrator must assign a userid, a CA-Top Secret ACID, and a password. (In most cases the userid and ACID will be the same.) If the signon procedure is different for new users, it is recommended that a separate signon procedure be outlined and a New User form be developed.

The New User form is used to notify central security that they must set up a new account. It must contain all necessary access requirements. A sample New User form can be found in the section "Sample User Guide".

Note: Care should be taken when assigning the userid and CA-Top Secret password. To ensure confidentiality, the assignment should be communicated directly to each

user by his security administrator. In addition, users must be informed of all password rules and regulations.

D.1.6 Password Procedures

Along with signon/signoff procedures, password rules and regulations should be listed in the user guide. Because CA-Top Secret offers an extensive variety of password controls, password usage strategies must be established as one of the first implementation procedures.

Whichever password policies are established by your company, it is imperative that the user be informed of all password rules and responsibilities. This can be done by establishing guidelines and providing users with the following password procedures:

- **First Password**

  An explanation of obtaining/creating a user's first password.

- **Changing a Password/Password Limitations**

  An explanation of how to go about changing one's password, including password rules such as minimum length, masking requirements, and restricted passwords.

- **Lost Password**

  A procedure that a user can follow if he forgets his password and cannot sign on to the system.

- **Expired/Aging Passwords**

  A procedure that informs the user of what to do if his password has expired or is about to expire.

When developing password procedures for your user guide, keep in mind the following CA-Top Secret control options which manage password operation: NEWPW, RNDPW, HPBPW, INACTIVE, PTHRESH, and RPW.

Password Guidelines: Users must be made aware that passwords are the means of controlling access to all user accounts and must be treated in such a manner as to prevent disclosure to unauthorized individuals. The following password guidelines should be tailored to fit your needs and presented in your user guide:

1. Memorize your password upon receipt.
2. All written records of our password should be destroyed.
3. Do not post your ACID or password near the terminal, disks, cabinets, bulletin boards, or other areas accessible to unauthorized individuals.
4. Do not maintain your password in an unprotected data set where others could view it.
5. Do not share your ACID or password with anyone. Personnel requesting the use of another's ACID or password should be directed to the appropriate security administrator.
6. Inform your security administrator immediately if you suspect that your ACID or password have been compromised and request a password change.

D.1.7 Requesting Resource Access

Every CA-Top Secret ACID is connected to a department and, optionally, to profiles or divisions. In turn, departments, profiles, and divisions are permitted access to various resources. In the event that access to an additional resource is required for a user to perform his job, he must follow a procedure to obtain access. It is recommended that a Resource Access form be developed for this purpose.

Sample Resource Access forms can be found in the section "Sample User Guide" later in this appendix and in Appendix C.

Emergency and Off-Hours Access Procedures: Special projects may require that a user be permitted access to a resource or facility immediately or during off-hours. The procedure or person to contact for emergency access should be referenced in the user guide.

D.1.8 Online Batch Job Submission

CA-Top Secret imposes no changes to JCL when submitted from ICCF, CA-Vollie, CICS, and other online facilities. Users should be aware that:

- Jobs will automatically be tagged with their ACID.
- Permission must be granted to submit a job on behalf of other users and a USER=ACID parameter must be inserted on the JOB card. Unauthorized job submissions will receive a CA-Top Secret message and the job will be removed from the queue.

Note: CA-Top Secret passwords should never be coded on a job card that is stored online, especially in a library that is shared among other users.

D.1.9 How to Report Security Problems

Users should be instructed on the proper way to report actual or suspected security problems. Problems include suspected misuse of ACIDs, unexpected violations, signon problems, ACID suspensions, and so on. Problem determination procedures should emphasize the following points:

1. Sign on and resource access violations are counted and a violation threshold is set. If the number of violations an ACID receives exceeds the set threshold, the ACID is suspended and the session is terminated. Therefore, users should not ignore CA-Top Secret violation messages and should not repeatedly try to sign on or access the resource.
2. When problems occur, CA-Top Secret or IBM messages will be displayed.

   If violation messages are displayed, do not clear the messages from the terminal (do not press any keys on the keyboard). The user should:

   a. Copy down all CA-Top Secret or IBM message numbers and accompanying text.

   b. Record all entries prior to receiving the messages.
3. The user should immediately report the problem to his supervisor.

D.1.10 CA-Top Secret Messages

CA-Top Secret displays four types of security messages. The messages are prefixed with TSS followed by three numbers and a letter indicating the type of message:

- Messages ending with A are action messages that require a user response. Most likely, operators will be the only users to encounter such messages.
- Messages ending with an I are informational messages, many of which are displayed during signon.
- Messages ending with E are error messages indicating that the user has not supplied the correct information.
- Messages ending with W are warning messages.

The user guide should list the most commonly occurring messages with a brief description of the meaning of each message. Below is a list of recommended messages. Detailed meanings can be found in the *Messages and Codes Guide*.

TSS7000I	TSS7011A	TSS7227E	TSS7110E
TSS7001I	TSS7191E	TSS7160E	TSS7141E
TSS7003W	TSS7220E	TSS7102E	TSS7143E
TSS0750A	TSS7221E	TSS07101	TSS7172E

D.1.11 Security Features

Every CA-Top Secret user can monitor security for himself using the following built in security features:

TSS LOCK/UNLOCK Users can lock an unattended terminal using the TSS LOCK command. To unlock a terminal the user must enter the TSS UNLOCK command and his signon password.

TSS Last-Used Message When a user signs on to a facility and the TSS FACILITY(LUMSG) control option is set, CA-Top Secret displays the Last-Used message (TSS7000I). This message tells the user when his ACID was last used and through which CPU and facility. It enables the user to detect illegal use of his ACID.

TSS Status Message If the FACILITY(STMSG) control option is specified, the user will receive the Status message (TSS7001I) upon accessing the system. This message provides the user with information as to how his session will be processed with regards to security. The message also contains a current count of the number of times the user has used his ACID for sessions to batch jobs.

TSS WHOAMI The TSS WHOAMI command can be entered by any user. When successfully executed, WHOAMI displays CA-Top Secret message number TSS0303I. This message contains information—such as a user's facility, terminal ID, system ID, and mode—that can be helpful when reporting possible security problems.

D.2 Sample User Guide

The material in this section is provided as a sample user guide for "ANY COMPANY". ANY COMPANY runs under the CICS facility and has implemented the use of New User and Resource Access Request forms. An example of each form appears below.

ANY COMPANY - REQUEST FOR NEW USER

User Name
_____

Dept/Div _____

Effective Date _____ to _____

User Access Class _____

Facility(s) _____

Userid Call extension 200.

First Password Call extension 200.

Approvals: SCA _____ DCA _____

ANY COMPANY - RESOURCE ACCESS REQUEST

Requester's Name _____ ACID _____

Dept/Div _____

Effective Date _____ to _____

Purpose of Request _____

Resource Type _____

Requested Access Level _____

Approvals: SCA _____ DCA _____

ANY COMPANY
CORPORATE DATA SECURITY

Security Policy & Structure

In an effort to protect this company's valued data processing resources, the CA-Top Secret data security product has been implemented. CA-Top Secret controls who can access what resources, and how and when those resources can be accessed. Each employee is responsible for maintaining security by:

- Keeping all accounts confidential
- Revising account passwords at regular intervals
- Notifying the appropriate person(s) if abuse of accounts is suspected; and
- Actively supporting all company security procedures.

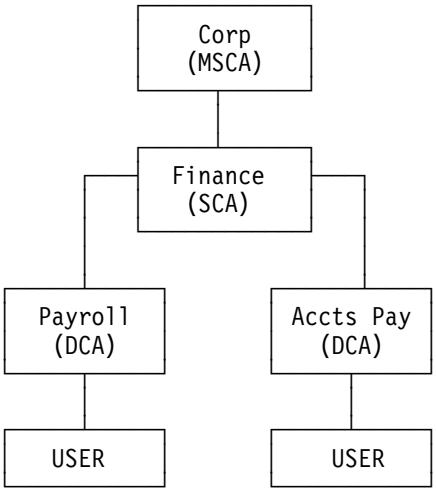
A copy of the Company Security Policy can be obtained through your supervisor.

Glossary

access	The way in which a resource can be used.
ACID	An acronym for ACcessor ID which identifies a user to CA-Top Secret; usually the same as your CICS userid.
error message	A system response that is displayed to tell you that the entered transaction was not valid; usually provides the reason why.
facility	The various subsystems supported by the central computer such as ICCF, CICS, and so on.
mode	The security implementation stage that determines how CA-Top Secret processes resource access requests. The four modes are: DORMANT, IMPLEMENT, WARN, and FAIL.
ownership	The state of being a protected resource. The owner of the resource has full access to it.
password	A unique string of characters associated with a particular ACID. Logon cannot be successful if an incorrect password is supplied.
permission	Authorization for access to an owned resource.
profile	A collection of identical resource permissions associated with a group of users performing the same job function.
resource	Something protected by CA-Top Secret, such as a data set, program, transaction, or terminal.
administrator	A person designated and authorized to grant users permission to access resources.
userid	Usually the same as your ACID.
violation	An illegal attempt to access a resource.

Security Structure

The following chart illustrates how this company's security is structured. You may want to jot down the name and extension of your immediate department security administrator.



Signon Procedures

Your security administrator has assigned to you a unique userid and password. Your userid/password combination identifies you to CA-Top Secret and allows you access to the resources required to perform your job. It is imperative that you safeguard your userid/password by following these guidelines:

1. Memorize your userid/password upon receipt.
2. All written records of our password should be destroyed.
3. Do not post your userid or password near the terminal, disks, cabinets, bulletin boards, or other areas accessible to unauthorized individuals.
4. Do not maintain your password in an unprotected data set where others could view it.
5. Do not share your ACID or password with anyone. Personnel requesting the use of another's ACID or password should be directed to the appropriate security administrator.
6. Inform your security administrator immediately if you suspect that your ACID or password have been compromised and request a password change.

New User Signon

If you are a new user, your security administrator will assign a userid/password to you via the New User form. The form will list your userid, a first time password, and the facility to which your userid is authorized. To sign on to the system the Standard Signon Procedure can be followed with the exception that your first time password will expire immediately. Read through the Standard Signon and Password Change procedures for your facility before attempting to sign on to the system. If questions arise, ask your supervisor for help.

CICS: Standard Signon

To sign on to CICS type:

CESN

Enter your CA-Top Secret ACID and your selected password.

Press Enter.

```
                Signon for CICS/TS Release 1.1.0      APPLID DBDCCICS

WELCOME TO  DBDCCICS          CLEAR SCREEN,ENTER CESN TO SIGNON



Type your userid and password, then press ENTER:

         Userid . . . .             Groupid . . .
         Password . . .
         Language . . .

     New Password . . .
```

CICS: Password Change

To change your password under CICS type:

CSSN 'NAME=*userid*,PS=*pswd/npswd*'***

Replace *userid* with your CA-Top Secret ACID; *pswd* with your old password; *npswd* with your new password.

Press Enter.

New Password Rules - CICS

The following rules apply when choosing a new CICS password:

1. Password must be four to eight characters in length.
2. At least three characters in your new password must differ from your previous password.
3. Password can be a mix of letters and numbers.

Expired/Aging Passwords

Approximately five days prior to the automatic password expiration date, CA-Top Secret will display the following message each time you sign on to a facility:

TSS7003W PASSWORD WILL EXPIRE SOON ON mm/dd/yy

where mm/dd/yy displays the month, day, and year that your password will expire.

Lost Passwords

If you should forget your password, CA-Top Secret will not allow you to access a facility. Do not attempt to guess your password. Notify your supervisor immediately. She will contact the SCA who is authorized to assign you a new password.

Reporting Problems

1. If violation messages are displayed, do not clear the messages from the terminal (do not press any keys on the keyboard).
2. Copy down all CA-Top Secret and/or IBM message numbers and accompanying text.
3. Record all entries you made before receiving the messages.
4. Report the problem immediately to your supervisor.

Requesting Resource Access

If CA-Top Secret is not letting you access a resource that is necessary to perform your job, inform your supervisor immediately. You or your supervisor must fill out a Resource Access Request form. Central Security will review your request and grant authorization.

Emergency Access

If a resource access is needed immediately, contact your SCA (ext. 200). SCAs are authorized to grant emergency access to a user on a limited time basis. To acquire unconditional access, a Resource Access Request form must be submitted.

Off-Hours System Access

Off-hour access is defined as non-business hours after 8.00 p.m. or before 6.00 a.m. during regular working days (including Saturdays) and at all times during holidays and Sundays.

Off-hour access will be granted when it is deemed necessary to meet business requirements. Contact your SCA. A minimum notice of 24 hours is mandatory.

CA-Top Secret Messages

TSS7000I acid LAST-USED date time SYSTEM=id FACILITY=fac

This message informs you when, on what CPU, and under which facility your ACID was last used.

TSS7011A PLEASE ENTER YOUR *NEW* PASSWORD

Your current password has expired and CA-Top Secret is requesting that you enter a new one.

TSS7221E DATA SET NOT ACCESSIBLE - dsname

An attempt was made to access the named data set to which you are not authorized.

TSS7227E ACCESS NOT GRANTED TO DATA SET

A requested function requires a data set access level you do not possess.

TSS7160E FACILITY facility NOT AUTHORIZED FOR YOUR USE

You are not authorized to access the named facility.

TSS7101E PASSWORD IS INCORRECT

The supplied password is not correct.

TSS7110E PASSWORD HAS EXPIRED. NEW PASSWORD MISSING.

Your current password has expired. You must supply a new password.

TSS7141E USE OF ACCESSOR ID SUSPENDED.

Your ACID is no longer valid due to an automatic or explicit suspension. Contact your supervisor.

TSS7143E ACCESSOR ID HAS BEEN INACTIVE TOO LONG

Your ACID is no longer valid due to inactivity. Contact your supervisor.

TSS7172E YOUR ACCESSOR ID IS ALREADY IN USE ON TERMINAL terminal-name

Your ACID is already signed on to the named terminal.

Multiple signons are not supported.

Security Features

You can monitor security using the following CA-Top Secret security features:

TSS LOCK/UNLOCK -
Use the TSS LOCK command to lock an unattended terminal. To unlock a terminal use TSS UNLOCK (you will be prompted for your signon password).

TSS Last-Used Message -
CA-Top Secret displays the Last-Used message (TSS7000I). This message tells you when, on which CPU, and through which facility your ACID was last used. It enables you to detect illegal use of your ACID.

TSS Status Message -
This message tells you how your session will be processed with regards to security. It also contains a current count of the number of times your ACID was used to submit batch jobs.

TSS WHOAMI -
TSS WHOAMI displays CA-Top Secret message number TSS0303I. This message contains information—such as your facility, terminal ID, system ID, and mode—that can be helpful when reporting possible security problems.

Index

R

S

T

U

V

User Registration Form

If you are interested in registering as a user of Computer Associates software, please complete the information below. Send it to the following address:

Computer Associates International, Inc.
ATTN: User Registration
One Computer Associates Plaza
Islandia, NY 11749

Registration entitles you to receive such items as:

- newsletters
- product release announcements
- information about User Groups
- information about CA conferences
- client questionnaires

You *do not* have to be the primary contact for CA software within your company or organization. All you have to be is interested in CA software, how it is used, and where it is headed.

Product(s): _____

_____

_____

_____

Site ID: _____
(Enter UNKNOWN if you do not know your Site ID.)

Name: _____

Position: _____

Company or organization: _____

Address: _____

Address: _____

Phone No.: _____

Date: _____

I would like additional information on: _____

Demand Analysis Request Form

Please use this form to make suggestions for product improvement. Send it to the following address.

Computer Associates International, Inc.
ATTN: Demand Analysis Requests
One Computer Associates Plaza
Islandia, NY 11749

Be sure to print your name and address below if you would like a reply.

Name: _____

Position: _____

Company or organization: _____

Address: _____

Address: _____

Phone No.: _____

Date: _____

Is DAR from a User Group? (Yes/No) ___ User Group ID: _____

Priority: _____

Description of Requested Item:

_____

_____

_____

_____

_____

_____

_____

_____

_____

CA Account Manager:	CA Office:
Input by:	Date:

Reader Comment Form

CA-Top Secret Planning Guide

Release 3.0 VSE

Document Number: R101TS30PLE

Please use this form to tell us how you use this manual and to make suggestions for improvement. Send it to the following address. (To request additional publications, call 1-800-841-8743 or check the CA home page (http://www.cai.com) on the Internet. To ask questions about the functionality of CA products, contact your CA representative.)

Computer Associates International, Inc.
ATTN: Reader Comment Form
One Computer Associates Plaza
Islandia, NY 11749

Be sure to print your name and address below if you would like a reply.

Name: _____

Position: _____

Company or organization: _____

Address: _____

Address: _____

Phone No.: _____

Date: _____

Years of experience with this CA product: _____

Overall Rating

	Good	Fair	Poor	Why?
Accuracy				
Organization				
Clarity				

Reference Aids

	Good	Fair	Poor	Why?
Contents				
Index				
Glossary				
Reference to Other Manuals				

Clarity

	Good	Fair	Poor	Why?
Instructions and Procedures				
Examples				
Graphics				

How Manual Is Used:

How do you use this manual in your job?

How often do you use this manual in a week?

Suggestions:

What do you like about this manual?

What do you dislike about this manual?

What would you like us to change?

Additional Comments: