CA Top Secret® for z/VM

Planning Guide

r12

Second Edition

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction 11

Objectives....11
Basis for the CA Top Secret Implementation Plan....11
CA Top Secret is a Means to an End....12
Implementation Requires Adequate Support....12
Security is a Global Concern....12
Security Implementation is Ongoing....12
Remaining Chapters....13

Chapter 2: Formulating a Security Policy 15

Statement of Goals....15
Gain Support For Security Implementation....15
Scope of Security Policy....15
Primary Elements of a Security Policy....15
Security Administration....17
Systems Software Area....18
Applications Software Areas....18
The Auditing Function....18
Operations....19
All Users....19
Levels of Security....19
Conclusion....20

Chapter 3: Security Administration Function 21

Description....21
Where to House Security Administration....21
Alternative Recommendations....21
Sampling of Locations....22
Any Port in a Storm....22
Establish a Backup....23
Centralized Security....23
Decentralized Security....24
Set-up/Maintenance Dependencies....24
Suggested Solutions....25
Security Administrator's Responsibility....25

Chapter 4: Assign Implementation Team 27

Suggested Team Members 27
Cooperation Essential 27
Project Team's Function 28
Develop Security Policy 28

Chapter 5: Develop Implementation Plan 29

Scheduling Implementation 29
    Construct a Flexible Schedule 29
    Consider Task Dependencies 29
Distributed Security 32

Chapter 6: Product Training 33

Learn the Basics 33
Knowledge is Power 34
    CA Education Services 34
CA-World 34
    Local User Groups 34
    CA User Conference 35
    Security Organizations 35

Chapter 7: Passwords and Password Phrases 37

About Passwords and Password Phrases 37
Password Control Options 38
Password Phrase Control Options 39
Random Password Generation 39
Prevent Password Changing 40
Prevent Password Phrase Changing 40
Password Attribute for ACIDs 41
Password and Password Phrase Expiration Intervals 41
Password and Password Phrase History 42
Required Password Controls 42
Conclusion 42

Chapter 8: Installation 43

Prerequisite Information 43
Select Control Options 43
Installation 45
CA Top Secret Start-up 45

Chapter 9: Backup and Recovery Procedures 47

BACKUP Control Option 47
Recovery Procedure 47
Operator Training 47
Candidates for Offsite Storage 48
Analysis 48
Objectives of the Inventory 48
Prioritize Users and Resources 49
CA Top Secret-Protected Resources 49
Organize Users into Groups 49
Take Inventory of Resources 49
Organize Resources 50
Assign Access Levels to Users/Resources 50
Record Assignments Online 50
Conclusion 50

Chapter 10: Naming Standards 51

Guidelines 51
Resource Naming Standards 51
User Naming Standards 51
Common Naming Standards 52
CA Top Secret Security File Standards 53

Chapter 11: Security File 55

Design 55
Security File Structure 55
Defining Department, Division, and Zone ACIDs 56
- Organization ACIDs Structure 56
- Defining Resource Ownership 57
- Defining Ownership to Master Security Administrators 57
- Define Ownership at High-Level Prefix 57
- Designing Profiles 58
- Define Job Requirements 58
- Design Options 58
- Group Design 60
- The ALL Record 61
- Defining Users 61
- Documentation of Security File Design 61
- The NAME Field 61

Chapter 12: Refine Security Administration Structure 63

Who Administers Security? 63
TSS Command 63
The MSCA 63
Physically Secure the MSCA's Password and ACID 64
Suspension of MSCA 64
Additional Central Security Administrators 64
Suggested SCA Authorities 64
Decentralized Security Administrators 65
ZCA, VCA or DCA Considerations 65
Password Viewing 66

Chapter 13: Develop Implementation Strategy 67

Phased Implementation 67
Implementation Options 67
Modes 67
Implementing Default Protection 70
Implementation by Facility 70
Protecting Special Resources 71
Minidisks 71
CPUs 71
Terminals 71
OS/DOS Data Sets and Volumes 73
SFS Command and Directory Protection 75

Chapter 14: Logging and Reporting Options 77

Logging Activity and Violations 77
Audit File 77
Reporting Activity and Violations 77
TSSCFILE 78
TSSREPT 78
TSSAUDIT 78
Generating Reports 78
Ad Hoc Reporting 79
User Message and Violation Suppression 79
Avoid Message Suppression 79
Logging and Violation Control Options 79

Chapter 15: Define Procedures for Handling Violations 81

Monitoring Discourages Violation Attempts 81
Elements of Procedure 81
Conclusion 82

Chapter 16: Plan Emergency and Troubleshooting Procedures 83

Production Security Violations 83
CA Top Secret Software Problems 83
Disaster Recovery 84
- If Installing Operating System at Site 84
- If Using the Site's Operating System 85
- Plan to Install Security 85

Chapter 17: Define Audit Requirements 87

Audit Requirements 87
Defining CA Top Secret Auditors 87
Defined as Administrators 87
Using CA Top Secret Auditing Capabilities 88
CA Top Secret Utilities 88
- TSSUTIL 88
- TSSAUDIT 88
- TSSCFILE 88

Auditing Users and Resources 89

Chapter 18: Define Security Maintenance Procedures 91

Security File Maintenance 91
Verifying Change Requests 91
- Maintenance Request Forms 92
- Proper Maintenance 92
- Design Procedure For Quick Turnaround 92

CA Top Secret Software Maintenance 92
- Reason for Software Maintenance 93
- Software Maintenance Considerations 93
- System Software Maintenance 93

Chapter 19: Develop Testing Procedures 95

Chapter 20: Customization 97

Common Reasons for Customization 97
- Virtual Machine Interfaces 97
- CA Top Secret Installation Exit 97
- Conclusion 98

Chapter 21: Develop Security Awareness Programs 99

About Security Awareness Programs 99
Goals of Awareness Program 99
Cultivate Cooperation 100
- Systems Software Area 100

Educate the Security System Users 103
- Subject Matter 103
- Training Development 104
- Communicate the Security Policy 104
- Security Seminars 105

Chapter 22: Schedule Ongoing Evaluation 107

Ongoing Evaluation 107
Evaluation Team 107
Team Responsibilities 107
Annual Security Review 108

Appendix A: Sample Security Policy and Maintenance Form 109

Human Resource Security Policy 109
- PURPOSE 109
- POLICY 110

Sample Maintenance Form 113

Chapter 1: Introduction

This section contains the following topics:

Objectives (see page 11)
Basis for the CA Top Secret Implementation Plan (see page 11)
Remaining Chapters (see page 13)

Objectives

This document provides guidelines that help you plan the effective implementation of CA Top Secret for z/VM. 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 organization. Recommendations are presented, along with tradeoffs, which you may 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.

After reading this guide, you should be able to:

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

Basis for the CA Top Secret Implementation Plan

As with any objectives, there are a set of conditions which must be understood prior to any attempt to meet the objectives. The implementation plan CA Top Secret at your installation must be based on the following premises:

- CA Top Secret is a Means to an End
- Implementation Requires Adequate Support
- Security is a Global Concern
- Security Implementation is Ongoing

CA Top Secret is a Means to an End

Your environment is not secure immediately after installing CA Top Secret. Rather, it 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 discussed 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 that consists 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 may find that your use of CA Top Secret must continually adjust to reflect changes that occur within your installation. Your CA Top Secret implementation is just as dynamic as your data processing environment. It requires continual analysis, review, and modification to properly protect your installation.

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 section contains the following topics:

Statement of Goals (see page 15)
Primary Elements of a Security Policy (see page 15)
Conclusion (see page 20)

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 statement of security objectives, can be developed before the implementation is begun.

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 stops 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.

Scope of Security Policy

The security policy might confine itself to addressing only those issues which relate 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.

Primary Elements of a Security Policy

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

- Objectives or premises that prove the need for security in your environment.
- Scope of security: What is to be protected (data, software, and hardware, etc.)?

- Ownership of resources: Who owns the data processing resources such as data, facilities, and hardware?
- Responsibility for the integrity of the resources: Who is responsible to ensure that resources are being accessed, used, or modified in a secure manner?
- 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.
- Statement of intent as to how violations are logged and reported.
- Accountability: What action is taken when security is breached?
- Account protection requirements: In password-based security systems, this may include change intervals, one account per employee, and account assignment for remote users. This assumes that:
  - Access to data processing facilities and data is company property granted to the employee to perform a specific job function.
  - Each employee is responsible for the use of their account.
- 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 resources must understand that they have a role to play in the security scheme, and must understand what that role is.

What follows is a discussion of the typical functional areas in a normal environment, and what their responsibilities include.

Security Administration

The central security administration area is 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:

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

Decentralized Security Administration

A statement on the appropriateness of decentralized security administration can be detailed in the policy. If it is included as a viable means of administration for the environment, responsibilities of the area must be detailed. Following are some of the typical responsibilities of a decentralized Security Administrator:

- To assist the central Security Administrator within the guidelines of the policy.
- To handle security administration requirements for the areas which fall within their scope.
- To assist in the development of security designs for all user requirements which fall within their scope.
- To report violations to the appropriate authorities and provide follow up activity on same.
- To document security controls which exist within their scope.

Systems Software Area

The systems software area is an area that must be considered critical in any organization. First, the security software is the responsiblity of this area. Moreover, systems software personnel often use facilities that are capable of bypassing or even disabling the security software. Given this exposure, the policy must detail the responsibilities of this critical area as it relates to security. Consider identifying the following responsibilities for systems software:

- 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.
- To notify the appropriate parties if the security software is disabled as soon as it is practical.
- To limit development and availability of facilities capable of bypassing security to only those situations in which they are absolutely necessary.
- To work with the security administration function to ensure that system resources are properly protected.
- To design the security requirements for the vendor-supplied system software which is their responsibility, and to work with the security administration area in implementing same.

Applications Software Areas

The applications areas must interface properly with the security areas to ensure that application resources are properly protected. Each application area is the best source of information concerning how best to protect an application, since each application differs to some extent. Consider the following responsibilities:

- To define the security requirements for the application, and to work with the security administration area in implementing security for the application.
- To notify the appropriate Security Administrator of all revisions to the application that affects the security design.

The Auditing Function

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

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

Operations

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

- To handle all responsibilities of production processing in a secure manner.
- 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.

All Users

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

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

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 is evaluated, in part, by their adherence to security policy, then it is generally understood that your organization takes security seriously.

Levels of Security

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

- Corporate Level
- 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 that this guide discusses.

Application Level

There are often applications that require additional measures above and beyond the level set by the corporate policy. Specific policies may 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.

Conclusion

There is a sample of an application level policy in the Appendix. This policy was submitted by a CA Top Secret customer as a suggested base for your security policy.

No matter which form the policy takes, the critical point in the security implementation is that direction be set and communicated before implementation begins. Without this direction, 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 expects them to do the same.

Chapter 3: Security Administration Function

This section contains the following topics:

Description (see page 21)
Where to House Security Administration (see page 21)
Alternative Recommendations (see page 21)
Establish a Backup (see page 23)
Centralized Security (see page 23)
Decentralized Security (see page 24)
Set-up/Maintenance Dependencies (see page 24)
Suggested Solutions (see page 25)
Security Administrator's Responsibility (see page 25)

Description

Establishment of the security administration function is one of the first things to be considered after direction has been defined. This chapter provides information which enables you to determine where security administration resides and who handles the function. This is 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 administrators are better equipped to handle the ongoing task if they are involved from the beginning of the implementation.

Where to House Security Administration

The security administration function can live anywhere within the organization. The singularly best place is in a security administration area which 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 must reside in an area where it has the power to enforce security. This power must be granted and actively supported by the top management of the organization. The area must also have the manpower available to staff the function. Under these circumstances, the security administration function can live virtually anywhere within an organization.

Sampling of Locations

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

- Systems Software Area: The systems software area is very involved with the security software itself.
- Data Base Management / Data Administration: Requests for access to corporate data are usually made to this area.
- Operations: They are responsible for all processing.
- Auditing: They are 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 resides.

After the functional area for security administration is selected, the next step is to choose the individual(s) who handle the function. The job of a Security Administrator is a tough one. The nature of the position forces the administrator to poke into every nook and cranny in the data processing environment. It is also a very responsible position that requires a strong personality. Some of the characteristics which you may consider in a potential Security Administrator are:

- Knowledge of data processing resources and appropriate security requirements
- Highly responsible
- Personality which commands respect and trust
- Good analytical and organizational skills
- Good political awareness of the environment
- Excellent interpersonal skills
- Nerves of steel, heart of stone, desensitized to insult or injury.

The classic quote is, “Nobody likes the Security Administrator.” To a large extent this is true because the administrator has a job to do which is not a popular one, at least not initially.

Establish a Backup

Incidentally, 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.

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).

After setting up the central security administration function, you must consider whether or not to centralize or decentralize the security function. There is no one correct answer to this question. There may be an answer as it relates to an individual environment, but only careful analysis determines what the solution is for your organization.

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

Centralized Security

Centralized security:

- Gives concentrated control over changes in security, and strengthen security enforcement
- Provides one point for security administration
- Makes policies and procedures simpler to develop, enforce, and monitor
- Provides a higher level of security by limiting the number and distance of individuals authorized to change security definitions
- Allows for more flexible reporting and
- Requires fewer security staff members than required by a decentralized organization.

But, centralized security might....

- Be less responsive to the user due to logical and physical distance from the user's environment
- Involve longer response times to react to maintenance requests
- Require a higher maintenance workload.

Decentralized Security

Decentralized security:

- Allows more sensitivity to user requirements since the administrator is more familiar with the resources being protected, and with the users, than is possible at the central level
- Allows faster response to maintenance requests
- Requires a lower administration workload per administrator since security maintenance is 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 is 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.

Set-up/Maintenance Dependencies

In any decision regarding who is to handle security administration, you must consider the amount of set-up and maintenance activity required.

This depends on:

- The number of corporate entities, for example, 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.
- 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 could be heavy.
- The application development activity. If heavy development is being pursued as in most installations, 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 same.
- The number of special routines requiring user-defined resources, and the maintenance activity against them.

Suggested Solutions

If maintenance activity is 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.

You can also centralize now and 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.

Security Administrator's Responsibility

The typical responsibilities of centralized and decentralized administrators were detailed in the "Formulating a Security Policy" chapter. In brief, Security Administrators must be responsible for implementing, maintaining, monitoring and enforcing security and the CA Top Secret security software.

Chapter 4: Assign Implementation Team

This section contains the following topics:

Suggested Team Members (see page 27)
Cooperation Essential (see page 27)
Project Team's Function (see page 28)
Develop Security Policy (see page 28)

Suggested Team Members

The security implementation requires 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.

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 Essential

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

Project Team's Function

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

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. This 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.

Chapter 5: Develop Implementation Plan

This section contains the following topics:

Scheduling Implementation (see page 29)
Distributed Security (see page 32)

Scheduling Implementation

Time frames can be established if the administrator has a good feel for the size of the task. But what is more often the case, is that 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 it is best to become generally knowledgeable of every system, applications and operations procedure, and facility in the shop. This is something that is not obvious until the inventory and design phases begin.

Construct a Flexible Schedule

To accommodate this "can of worms," the implementation team can 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, implementation progresses smoothly, and speeds 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 time frames on each phase of the implementation plan, as it is to be certain that the implementation tends to all requirements.

Consider Task Dependencies

Create a task list or flowchart showing all tasks that must be accomplished to implement security at your site. This allows 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 that may be listed are outlined below.

Security Plan Components

The following tasks may 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 document.

- 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 cause 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 must accompany this task because once CA Top Secret is installed, your installation may 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 is 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 must 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 schedule a task to address the development and implementation of standard resource names. The existence of standard resource names can expedite the implementation process, and results in a clearer, less complicated Security File.
- Security File Design—The results of the inventory can give you an organized picture of the users and resources and how they relate to each other. This input can be used in designing the Security File. It is important to schedule the time to design the file before actual administration begins. This simplifies the maintenance effort later on.
- Definition of Implementation Strategy—Each organization may choose to approach the implementation in a different manner, addressing different resources and using different options and controls. A task can 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 are logged, reported, and handled. A task can 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. For this reason, it is critical to schedule the time to develop emergency procedures which help minimize the time required to diagnose and resolve specific problems before they occur.
- 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 require changes to the Security File. Also, upgrades in the operating system may result in upgrades to the security product itself. CA Top Secret also periodically upgrades and adds features and facilities. Development of maintenance procedures may be scheduled early on in anticipation of subsequent maintenance requirements.
- Testing—A test plan can be designed to ensure that the security product is implemented and functioning as desired in the installation. You may find that testing is a function that continues ad infinitum as the package is enhanced and as your use of the package evolves into more elaborate security controls. A good test procedure can developed that remains useful long after 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 automatically address. In this case, customization is necessary. This task must 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 depends on the support of the user community. Support comes only if the users are properly educated in the features of the security product. This is an important phase which may be time-consuming, but cannot be ignored since security enforcement ultimately comes 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 can be developed and scheduled at regular intervals. This ensures that CA Top Secret is used properly and effectively.

Distributed Security

In a traditional, centralized environment, all processing is performed on the same system whether it is a mainframe, mid-range, or PC. Many installations, however, in order to remain competitive, have chosen to decentralize their operations and to diversify both their hardware and software packages. CA Top Secret VM, through the use of distributed security processing, allows these environments to continue maintaining the security and integrity of their data across multiple platforms without having to commit to extensive retraining.

Distributed security in CA Top Secret coordinates multisystem security by using the CA Common Communication Interface (CAICCI). CAICCI standardizes communication within connectivity software, thus enabling CA Top Secret to integrate individual security processes on different platforms.

An important part of distributed security in CA Top Secret is the Command Propagation Facility (CPF) which can route security administration to all or selected nodes either synchronously (CA Top Secret will wait for a response from each targeted node) or asynchonously (CA Top Secret will not wait for a response from each targeted node), resulting in single point administration. Changes made to ACIDs, passwords, or access levels, for example, can be propagated to all nodes to which the user is defined. Through the use of the CPFNODES, CPFWAIT and CPFTARGET control options, CPF defaults can be tailored to suit the needs of a particular security administration and policy.

Chapter 6: Product Training

This section contains the following topics:

Learn the Basics (see page 33)
Knowledge is Power (see page 34)
CA-World (see page 34)

Learn the Basics

It is recommended that you become familiar with the following information:

- Installation: how CA Top Secret interfaces with the operating system.
- Default Operation: how CA Top Secret behaves by default.
- Control Options: the different options available to change the way CA Top Secret functions. These include options in the following areas:
  - Security System Logic Options
  - Security State of Awareness Options
  - Security Activity Logging Options
- System Architecture: the basic operational design.
- Security Administration Functions as provided by facility and by limiting scope.
- CA Top Secret implementation strategies.
- Auditing Functions.
- Logging and Reporting Functions.
- Automated Backup Functions.
- Recovery Functions: what to do when CA Top Secret is sick. The following questions may also be considered:
  - How does CA Top Secret tell you that it is sick?
  - What does CA Top Secret do when it is down?
  - Under which circumstances does CA Top Secret die?
  - What kind of security is available if CA Top Secret is sick?

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 behaves and how it works for you. If you do not, you run the risk of being in a situation where it controls 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.

CA Education Services

CA Education offerings include instructor-led and computer-based training, product certification programs, third-party education programs, distance learning, and software simulation. These services help to expand the knowledge base so you are better able to use our products more efficiently, contributing to your greater success. CA Education has been developed to assist today's technologists in everything from understanding product capabilities to implementation and quality performance. Contact your account manager for brochures, descriptions, and schedules of available seminars.

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.

Local User Groups

There are local 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.

Contact your account manager for more information on CA Top Secret user groups.

CA User Conference

Users of all CA products meet annually to share ideas on new enhancements, features, etc. For more information contact your account manager or refer to the CA-Client Support Handbook.

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: Passwords and Password Phrases

This section contains the following topics:

About Passwords and Password Phrases (see page 37)
Password Control Options (see page 38)
Password Phrase Control Options (see page 39)
Random Password Generation (see page 39)
Prevent Password Changing (see page 40)
Prevent Password Phrase Changing (see page 40)
Password Attribute for ACIDs (see page 41)
Password and Password Phrase Expiration Intervals (see page 41)
Password and Password Phrase History (see page 42)
Required Password Controls (see page 42)
Conclusion (see page 42)

About Passwords and Password Phrases

Passwords control access to user accounts in your organization. Unless you have devices to provide additional levels of user authentication (for example, voice or image recognition), passwords are the only means of providing user account protection for your environment.

In addition to a password, ACIDs can also have an optional password phrase for applications that support them.

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

The key to an effective password strategy is to choose controls that allow users to easily remember their passwords so that the passwords are not written down, but are not easily guessed.

Password Control Options

The following control options control CA Top Secret password operation:

INACTIVE

This option defines the number of days before CA Top Secret denies use of an ACID with an expired password. This option is inactive by default.

CA recommends that this option be used to deter use of ACIDs with expired passwords. 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 typically set at 30 days.

NEWPW

This option defines the new password rules that are 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.

PTHRESH

This option sets a password violation threshold, which when exceeded, suspends the user. The threshold count begins from the last successful sign-on. As you increase the threshold, password guessing by unauthorized users has a greater chance of success.

Default: 3

PWEXP

This control option specifies a password expiration interval that, in effect, becomes the default interval for the installation. Changing the expiration interval has no effect on current users; only on those created after the change.

PWHIST

This control option specifies how many passwords are retained in history to ensure that users do not reuse common passwords.

Range: Up to 64

PWVIEW

This control option suppresses 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.

RPW

If you prevent users from entering new passwords prefixed in the restricted password list (RS suboption of the NEWPW control option), you can add additional restrictions to this list. This option allows you to modify the restricted password list. You can include prefixes specific to your organization, such as, corporate names or acronyms. This option restricts attempts at password guessing by restricting passwords that may be common to your organization.

For more information, see the *Control Options Guide*.

Password Phrase Control Options

The following control options control CA Top Secret password phrase operation:

NEWPHRASE

Specify the controls for password phrase.

NPPTHRESH

Specifies the maximum password phrase violation threshold.

PPEXP

Specifies a password phrase expiration interval.

PPHIST

Specifies the number of previous password phrases maintained as part of an ACID's password history.

PPHRASE

Globally allows all users to specify a password phrase.

PPSCHAR

Adds, replaces, or removes characters from the password phrase valid character list.

For more information, see the *Control Options Guide*.

Random Password Generation

This option lets you select random password generation so that it might 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 are not easily guessed.

Drawbacks to this feature are:

- When generated, the random password is displayed on the user's screen and might be viewed if the terminal screen is not protected from casual viewing.
- Randomly generated password are not easily memorized. A user might write it down and compromise security.

CA recommends that if you use the random password feature, password masking be used to create a password that is potentially pronounceable. This helps the user to remember the password without writing it down.

Prevent Password Changing

The NEWPW option prevents 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
- 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 never changes

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

Prevent Password Phrase Changing

The NEWPHRASE(NU) suboption prevents users from changing their password phrases. Potential problems from selecting the NU suboption are:

- The CA Top Secret security administrator must change all user password phrases at the interval specified for each user
- The revised password phrases must be communicated to the users at the specified intervals, risking regular compromise of password confidentiality

If you prevent users from changing their password phrases and you also enforce password phrase change intervals, develop a secure communication procedure to ensure that users receive their own password phrase.

Password Attribute for ACIDs

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

password

Specifies a password for a user ACID to be used the next time the user signs on.

NOPW

Specifies that an ACID does not require a password. CA recommends that this 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

Specify the interval at which a password must be revised. The user is 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 expires the password the first time the associated ACID is used. This establishes and encourages confidentiality of passwords as quickly as possible. CA recommends that organizations choosing to allow users to change their own passwords use this parameter whenever passwords are created or replaced so that the administrator will not know what the password is after the user first uses the ACID.

Password and Password Phrase Expiration Intervals

To change the expiration interval, use:

- The PWEXP control option for a password
- The PEXP control option for a password phrase

Changing the expiration has no effect on current users, only on those who have been created after the change.

Password and Password Phrase History

The PWHIST control option specifies how many previous passwords are retained in history. Up to 64 passwords can be specified.

The PPHIST control option specifies how many previous password phrases are retained in history. Up to 64 password phrases can be specified.

Required Password Controls

CA Top Secret automatically records a history of the three prior passwords and uses this history in password change verification. A user is not allowed to change a password to a new password equal to any of the three prior passwords. In fact, a user cannot create a new password that is similar to any of the three prior passwords. Note that this checking is not done when an administrator replaces a password and the replacement does not update the password history.

This feature can be included in your password strategy and communicated to your user community.

Conclusion

Do not develop password and password phrase requirements before you have studied the options available with CA Top Secret. Organizations that have invested much time in developing 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 controls available to you with CA Top Secret.

After you have defined your password and password phrase requirements, you may wish to detail the controls in your security policy as the means of communicating these to your users

Chapter 8: Installation

This section contains the following topics:

Prerequisite Information (see page 43)
Select Control Options (see page 43)
Installation (see page 45)
CA Top Secret Start-up (see page 45)

Prerequisite Information

Before installing CA Top Secret, it is recommended that you read the following manuals:

- General Concepts
- Installation Guide
- Control Options
- Planning

Note: Familiarity with the *Implementation* guide is also beneficial.

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 behaves even if you choose to install CA Top Secret with default control options. In most cases, you may choose to alter some of the defaults when you first install CA Top Secret.

The control options detailed below must be given special consideration before installation. These options generally affect CA Top Secret operation and must be reviewed for default operation. In addition to the general comments below, you can review the Control Options guide and the Implementation guide to thoroughly understand the effects of these options.

AUDFILE

This control option identifies the data set name of the Audit File.

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 may not be changed because it may change how your CA Top Secret definitions are searched. If changed, it may result in valid access against resources that were thought to be restricted. Careful thought must go into the setting of this option.

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.. It is recommended that you use the automatic backup feature to allow for quick recovery of the Security File.

BKPFILE

This control option identifies the data set name of the Backup File.

DATE

This control option allows you to 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.

DOWN

The DOWN control option controls security for tasks initiating while CA Top Secret is down. The default allows the VM facility to revert to normal security while its address space is down. The DOWN option takes effect in all modes except DORMANT. 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 server 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. This is the first phase in a gradual CA Top Secret implementation.

RECFILE

This control option identifies the data set name of the Recovery File.

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 the RECFILE option is included in the CA Top Secret Parameter File. Include the RECFILE option in the CA Top Secret Parameter File if you intend to use the CA Top Secret Security File recovery procedure.

SECFILE

This control option identifies the data set name of the Security File.

Installation

After you have selected your start-up 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 do not install during peak production periods. However, as long as you have set the MODE control option to DORMANT, CA Top Secret does not impact your operation after installation, but gives you the capability to use the TSS command for security administration.

CA Top Secret Start-up

It is recommended that the autologging of the CA Top Secret server machine be added to the tasks performed by the installation's AUTOLOG1 virtual machine.

Chapter 9: Backup and Recovery Procedures

This section contains the following topics:

BACKUP Control Option (see page 47)
Recovery Procedure (see page 47)
Operator Training (see page 47)
Candidates for Offsite Storage (see page 48)

BACKUP Control Option

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 file daily, at 1:00 a.m. by default. 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 control option. Review the Control Options Guide for the use and syntax of the BACKUP control option. In a shared environment, a backup is only active on one system.

Recovery Procedure

CA Top Secret also includes a recovery mechanism based on the DASD backup and the Recovery File. This procedure is implemented and tested before serious security maintenance begins so that all Security File updates can be recovered. See the *Implementation Guide* for further details.

It is strongly 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.

Operator Training

When setting up the backup and recovery procedures, you may 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.

Candidates for Offsite Storage

As with all critical files used in your installation, all of the following CA-Top Secret files must be backed up to tape daily, and may be candidates for offsite storage:

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

Offsite storage protects these files if your data center experiences a major disaster.

We recommend that the Security File reside on a different volume and string than that of the Backup and Recovery Files. This allows you to use the Backup and Recovery Files to quickly and easily circumvent minor hardware problems that affect access to the Security File.

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 is the best source of information on the resources required for their needs.

It is recommended, if the size or complexity of your organization warrants, that you address the inventory in manageable segments. This chapter provides guidelines for this analysis, and introduces several tools which make the task easier and more effective.

Objectives of the Inventory

The inventory and exposure analysis answers the following questions:

- Who are the users?
- What are the resources and must they be classified?
- Who is responsible for the resources?

- Which users are accessing which resources?
- Which users must access which resources to accomplish their job function, and at which access level?
- Which operations and procedures leave critical resources exposed?

Prioritize Users and Resources

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

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

CA Top Secret-Protected Resources

CA Top Secret protects the resources of virtual machines, data spaces, shared file systems and APPC connections, from logon until logoff.

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 VM directory class assignments. The results of the user inventory are input to the department and division design discussed in the “Design Security File” chapter.

Take Inventory of Resources

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

- VM directory for minidisks and links for data, and special devices for DIAL protection
- VTAM tables and the System Configuration file for available terminals
- RSCS node configuration files.

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
- The purpose of the resource.

Remember that CA Top Secret supports OS/DOS data set and minidisk 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.

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 is specific input to resource ownership decisions and design of profiles which you may perform. See the “Design Security File” chapter for more information.

Record Assignments Online

Recording your inventory results in an automated fashion possibly using an online editor. For example, XEDIT may serve you in later converting this information into the required TSS commands. In fact, it saves you time to record the results of your inventory in TSS command format.

Conclusion

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

Chapter 10: Naming Standards

This section contains the following topics:

Guidelines (see page 51)
Resource Naming Standards (see page 51)
User Naming Standards (see page 51)
Common Naming Standards (see page 52)
CA Top Secret Security File Standards (see page 53)

Guidelines

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 becomes much easier since you are able to use CA Top Secret's minidisk and data set prefixing or masking capabilities to define resources. This relieves you from having to define each individual resource, by allowing you to group resources together by prefix or pattern.

If you are implementing security in an organizations that has not enforced standards, or if you have no standards at all, your implementation may be more complicated because you may have to create more resource definitions.

Resource Naming Standards

Once the resource/user inventory has been completed 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.

User Naming Standards

CA Top Secret implementation is a good time to review your user ID naming standards. Many installations find that they have used different standards for each facility. Some organizations find that they have generated user names randomly, without following any pre-defined standard.

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 is being used.

Common Naming Standards

There are many theories on the development of user IDs:

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 allows you to trace the events associated with this user historical.

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 that identifies the employee, such as employee name or number.

Dynamic User IDs

The opposite of the preceding approach is to choose an ACID that identifies the department or location of the user by ACID prefix and identifies the user with a unique ACID suffix. This type of ACID may 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 User IDs

A common theory is to obscure the user ID so that an interested third party cannot easily guess it. 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 may 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.

CA recommends that you determine your approach before you begin to build your Security File and define your users.

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 must 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, or a security administrator.

Chapter 11: Security File

This section contains the following topics:

Design (see page 55)
Security File Structure (see page 55)
Defining Department, Division, and Zone ACIDs (see page 56)

Design

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.

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 the "Develop Naming Standards" chapter.
- 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 simplify maintenance and help you find a file element quickly when you need it.

Security File Structure

Most organizations base the 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 following illustration.

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

Defining Department, Division, and Zone ACIDs

CA recommends 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.

Organization ACIDs Structure

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

Examples

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 DIVISIONs and DEPARTMENTs to resolve the unique requirements of different corporate entities.

Do Not Delay File Design

It is often tempting to ignore designing a file structure as a first step in creating the 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 that results a file design without any real structure or forethought.

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). CA recommends that ownership be defined at this level for two reasons.

- Ownership of resources at the user equates to default access that cannot be overridden. Therefore, fine-tuning of access requirements for a specific resource cannot be done for the user 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.
- 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.

Defining Resource Ownership at Department/Division Level

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 that include masking characters.

Define 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 minidisks, try to define ownership by the high level prefix. This simplifies and reduces the number of required CA Top Secret ownership definitions.

Example

If USER01 has the following three minidisks:

```
USER01.0191, USER01.0291, USER01.0391
```

Then, assign ownership of USER01., not of USER01.0191.

Note: The VM resource, DIAGNOSE, does not honor generic prefixing.

Designing Profiles

Profile ACIDs are used to group together access requirements that are common to more than one user.

Define 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 which detail which users require access to which groups of resources, as input to your profile design.

Design Options

Consider the following options in designing your use of profiles.

Attach Profiles to Departments

Design your profiles such that all users assigned to a department are attached to profiles that are assigned to that same department. Profiles must be defined in departments.

Example: Profiles attached to departments

In this example, the applications department requires certain access to system resources. PROFILEX, which is attached to the applications department, contains those access requirements for the system resources. Therefore, to allow all application department users to access system resources, attach PROFILEX to the user ACID of each user via a TSS ADD or CREATE command.

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

PROFILEZ, which is attached to the Systems department, contains the access requirements for the system resources used by the Applications department users. To allow Applications department users to access the systems resources, attach them to PROFILEZ via an ADD or CREATE command:

Define Profiles By Application

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

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: override strategy

PROFILEA can be defined to allow READ access to system minidisks. PROFILEB can be defined to allow UPDATE access only to a critical subset of minidisks defined by PROFILEA. A user attached to PROFILEB and PROFILEA in the following order, has UPDATE access to the critical minidisks, and READ access to the remaining minidisks, where the access has not been overridden by PROFILEB.

```
PROFILEB
PROFILEA
```

Additionally, other users who only require READ access to system minidisks can simply be attached to PROFILEA.

Due to this override capability, profiles are always attached to users in the order ranging from the profiles that are most specific to their particular needs to the profiles containing the more general access requirements, since the specific ones override the more general.

Define Profiles By Job Description

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

Example: Profile by job description

A payroll clerk's job is always defined by PROFILEP while the payroll manager's job is defined by PROFILEM. Although the payroll clerk and the payroll manager might share common access requirements, they may nonetheless have individual profiles. This approach makes it 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.

Department/Division 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 can attach these profiles to your users as they are created and are associated with specific departments. When later requirements surface that affect users on the department or division level, you can effect these requirements simply by updating the appropriate department or division level profile.

Note: Profiles cannot be attached to divisions. To affect division level profiles, create a divisional department, to which no users are attached, and create your divisional profile within this department.

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. CA recommends 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.

Group Design

A group is similar to a profile in that it is a collection of users. The difference between profiles and groups is that groups are recognized by IBM OpenVM.

Each User ACID must be associated with at least one group if that particular group is recognized by IBM OpenVM.

When creating and using groups:

- You can attach a maximum of 254 groups and profiles to one user.
- You can’t assign a password to a group.
- You can’t attach a group to another group. A group must be attached to a department and a user.
- To attach a group to a user, *both* the ACID and the group must be within your scope of authority.
- Groups cannot own resources.
- Users can be assigned to a group permanently or temporarily.

The ALL Record

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

Your Security File design for FAIL mode, when all users are defined to CA Top Secret, indicates limited use of the ALL Record. Only truly global requirements are defined to the ALL Record. For example, the system disks required for CMS and commonly used CP commands, such as QUERY and BEGIN.

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 greatly simplify the actual definition of users to CA Top Secret.

Defining Users to Departments

Creating users is a rote exercise since all the pieces are in place to describe the proper environment for each user.

Documentation of Security File Design

Ddocument your Security File design, and what you have intended with this design and approach.

The NAME Field

The NAME field of the TSS CREATE command provides you with 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 above. It may be useful to develop a Security File dictionary that details for you each ACID by name, its purpose, and the nature of its use.

Chapter 12: Refine Security Administration Structure

This section contains the following topics:

Who Administers Security? (see page 63)
TSS Command (see page 63)
The MSCA (see page 63)
Additional Central Security Administrators (see page 64)
Decentralized Security Administrators (see page 65)
Password Viewing (see page 66)

Who Administers Security?

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, especially 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.

TSS Command

The TSS command, which is the tool for CA Top Secret administration, is easy to use. The administration menus can make administration even easier. You can further simplify maintenance by customizing these menus based on your individual requirements. 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.

The MSCA

The Master Security Control ACID or MSCA 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 use to initially accomplish this.

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

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 is used only when required. For example, only the MSCA can create SCAs so the MSCA account must be used for this purpose.

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. 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. See the *Control Options* guide for more information on the MSUSPEND control option.

Additional Central Security Administrators

At least one SCA must be created as the ACID used to perform routine maintenance. There is no limit to the additional SCAs 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.

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 and LSCAs can be created with reduced authority to handle specific environmental requirements. For example, some organizations create an SCA or LSCA with the authority to only suspend and unsuspend users. This ACID is assigned to an operator along 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.

Decentralized Security Administrators

Decentralized security is effected 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 the "Design Security File" chapter, 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.

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.

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 simply 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 13: Develop Implementation Strategy

This section contains the following topics:

Phased Implementation (see page 67)
Implementation Options (see page 67)
Implementing Default Protection (see page 70)
Implementation by Facility (see page 70)

Phased Implementation

Most organizations choose a phased approach to their implementation, especially if the organization must protect a variety of users and resources in different facilities. Even a small organization may choose a phased implementation strategy in order to address the implementation in manageable segments.

Organizations generally address the implementation by facility because each facility has different considerations and concerns. It is recommended that you initially organize your implementation effort into manageable segments. This ensures that you do not overwhelm yourself, or your security implementation team, with the full implementation effort all at once. The implementation can follow the same strategy that you have used in performing your user and resource inventory.

Implementation Options

CA Top Secret provides options which allow you to easily accomplish your phased approach to implementation. It is recommended that you review these options before planning your strategy.

Modes

As you have studied in *General Concepts*, there are four modes of implementation available with CA Top Secret. These modes can be assigned to the installation, to a facility, to a profile, to a user, or to an event. This allows you great flexibility in designing your implementation strategy. Because of this flexibility, you can easily find yourself in the middle of a very complex implementation if you do not take the time to review your options and plan your strategy accordingly.

DORMANT Mode

The first mode used in any implementation is DORMANT mode. This is the recommended mode in which to introduce yourself and your organization to CA Top Secret by inputting your Security File structure through the TSS command without affecting users' access to resources. Once you begin to define users, and you wish to bring them under CA Top Secret control either for research or for actual protection, it is time to choose one of the implementation modes: WARN or IMPLEMENT.

WARN Mode

WARN mode provides an excellent tool to determine which users are accessing which resources, or to test the access definitions that you have made in DORMANT mode. As with any other mode, you can set WARN mode for the entire installation or for the subset of the organization that you wish to test. Thus, WARN mode can be set by facility, by profile, or by user. In WARN mode, CA Top Secret does not stop violations, but CA Top Secret logs those violations and optionally sends violation messages to the user.

Signon Violations

WARN mode basically emulates FAIL mode in that all users must be defined to CA Top Secret or violations are generated. WARN mode does not prevent an undefined user from signing on, but it generates and records signon violations.

Password Violations

WARN mode does not prevent a defined user from signing on with an incorrect password, but it generates a password violation for that user. It is recommended that you set the WARNPW suboption of the FACILITY control option. This forces a defined user to supply a correct password in WARN mode.

Note: Security Administrators must always supply a correct password, even in DORMANT mode.

If you attach the DEFPROT attribute to specific resource classes, WARN mode records violations for all those resources that have not been defined. See Implementing Default Protection for a more thorough discussion of this approach.

Global WARN Mode: It is possible, but unusual, for an organization with multiple facilities to choose an implementation strategy which includes installation-wide use of WARN mode. Since all users must be defined to avoid violations, only a small organization might choose to take this approach. WARN mode is most often used to test segments of the implementation, or to back off from FAIL mode when an implemented segment of the organization is in trouble.

IMPLEMENT Mode

IMPLEMENT mode allows you to combine DORMANT and FAIL mode easily in your implementation strategy. All resources which have been defined to CA Top Secret or protected by default cannot be accessed by undefined users unless permissions have been defined to the ALL Record. Access to unprotected resources by users is treated the same way in IMPLEMENT mode as in FAIL mode (except for those resources which are protected by default only in FAIL mode). Unauthorized access attempts by defined or undefined users are failed.

Many organizations use a global IMPLEMENT mode strategy during implementation and override that mode where appropriate by facility, profile, user, or event.

If you attach the DEFPROT attribute to specific resource classes, IMPLEMENT mode records violations for all those resources that have not been defined. See Implementing Default Protection for a more thorough discussion of this approach.

FAIL Mode

Your implementation goal is to put your entire installation in FAIL mode. Your implementation strategy may include a gradual migration by segment to FAIL mode.

Mode by Event

Mode by event can be effected through the ACTION parameter on the TSS PERMIT command, or through the DRC control option.

ACTION Parameter

Allows you to put a specific permission in FAIL mode no matter which mode the user is in. This allows you to protect critical resources from users who are in the implementation process but are not yet in FAIL mode, or from undefined users. It can also enforce the use of VMPRIV in DORMANT mode.

The ACTION parameter also allows you to specify what access rights are authorized for QUERY and other such ambiguous commands by using the VMPRIV operand. For more details refer to the General Concepts Guide.

VMUSER Parameter

Allows you to apply VMPRIV to certain commands so that when executed they affect a specific VM userid. For more details refer to the General Concepts Guide.

DRC Control Option

Allows you to specify that selected violations, if incurred, always fail the attempt. This allows you to fail specific unauthorized access attempts even if the user is in DORMANT or WARN mode.

Implementing Default Protection

You can effect full default protection for specific pre-defined resources in the Resource Descriptor Table (RDT) Record by attaching the DEFPROT attribute to the particular resource using the TSS REPLACE(RDT) command function.

For example:

```
TSS REPL(RDT) RESCLASS(VMMDISK) ATTR(DEFPROT)
```

This TSS command function secures default protection for all minidisks, and provides flexibility in choosing the resources (minidisks, diagnose instructions, CPUs, etc.) that you want to protect.

You may regret giving every resource full default protection because you may find there are many resources in your organization that do not require protection.

Note: You can also dynamically define new resource classes to the Resource Descriptor Table, and, in turn, give them default protection. For more details, see the *Command Functions* guide.

Implementation by Facility

Since each VM facility used in your organization has different implementation considerations, it is recommended that you address them separately. You may find that each facility has special resources, and may have a completely different base of users. This becomes obvious when you have begun to address your user and resource inventory.

If your implementation task force can accommodate it, you might wish to address multiple facilities concurrently with different team members assigned to different facilities. This approach requires good communication and planning so that each facility implementation complements the others and so that users affected by more than one facility are getting consistent information and instruction from the different members of the implementation task force.

CA Top Secret allows you to select modes by facility, therefore, you can choose whichever approach suits your environment. As you progress, you can migrate the fully implemented facilities to FAIL mode while the other facilities remain in DORMANT, or in one of the implementation modes. Once again, you have tremendous flexibility in planning your implementation, and you may study your options before you proceed.

Protecting Special Resources

Certain resources require special considerations because of the nature of the impact they may have on your environment. For this reason, it is recommended that you have most of your implementation in place before you address these resources.

Minidisks

With the advent of VM/XA, four-digit virtual device addresses have been introduced. You should be aware that this change can cause some ambiguities in your PERMITs if they are not properly defined. For example, the following permission means USER01 can access USER02's minidisks ranging from 1900 through 19FF.

```
TSS PERMIT(USER01) VMMDISK(USER02.19)
```

While, means USER01 can access USER02's minidisks ranging from 0190 through 019F.

```
TSS PERMIT(USER01) VMMDISK(USER02.019)
```

CPUs

CPU control can be very effective for restricting access to CPUs in your shop. Once you have defined a CPU or all CPUs by prefix, no user is able to sign on unless they are specifically permitted to access the CPU.

CPU control must be carefully designed and planned before implementation to ensure that you do not unwittingly lock your users out of accessing the systems they need to do their job.

Note: If the DEFPROT attribute is attached to the CPU resource class, all CPUs are protected by default.

Terminals

CA Top Secret allows you to protect terminals so that they can only be accessed by authorized individuals. While this is often a popular implementation strategy, global terminal control often poses administrative problems that surpass the value that you might receive from terminal control.

Note: If the DEFPROT attribute is attached to the TERMINAL resource class, all terminals are protected by default.

CA Top Secret Protects Ports Not Hardware

When protecting terminals, you are not protecting the physical hardware device. You are protecting the port through which the terminal is defined to your system. It does not matter which actual physical device is attached to that port. The name of the port that you protect is defined and can be changed by your network control area.

This can be the cause of administrative problems. If you choose to protect all, or a significant number, of terminals in your organization, you must have solid procedures between the network control area and the security administration area to ensure that the security administration area is notified of every planned change to the network. This gives the security administration area time to redefine the affected terminals to complement the network change so that appropriate security is in place when the network is reconfigured.

Limit Protection to Critical Terminals

It is recommended that you limit the number of terminals protected to those that are truly critical, such as dial-in ports, production scheduling ports, or end-user ports for sensitive applications. This may make your terminal maintenance more manageable.

Remember, CA Top Secret architecture is based on the user, and it is the user who is responsible and accountable for their actions no matter which terminal is used to access your corporate resources.

Source

Source control allows you to restrict users to specific terminals. You may not be required to restrict most of your users to specific sources of entry. There may be a critical subset of your users for which this control may be appropriate, such as production schedulers or end-users using sensitive applications.

The same considerations given to terminal protection must be given to source control because you are defining the port as the source of entry. Again, it is critical to coordinate network reconfigurations between the network control area and the security administration area or unsuspecting users may come in to work one day only to find that they can no longer sign on to their terminals.

Source control, like terminal control, must be used selectively, to avoid large maintenance problems.

Note: The terminal ID of AUTOLOG restricts the use of a virtual machine in two ways: first, with a SOURCE(AUTOLOG) the ACID must be autologged; and secondly, it may not go through the usual procedure for signon. Ownership of terminal AUTOLOG does not allow the ACID to be autologged unless permitted to TERMINAL(AUTOLOG).

Terminal Locking

Unattended terminals can be protected against unauthorized access through the terminal lockout option. Terminal locking prevents use of the terminal until it is logged off, disconnected, or unlocked. Terminal locking can be triggered either automatically by CA Top Secret or through a user-initiated command.

A user can lock their own terminal by entering the TSS LOCK command function. To unlock the terminal, the user enters the TSS UNLOCK command function with his correct signon password.

Illegal attempts to UNLOCK a terminal increment the password violation count and result in action taken based on the PTHRESH option.

TSS LOCK/UNLOCK commands are ignored when issued by a disconnected virtual machine.

Automatic Locking

CA Top Secret will automatically lock a terminal that has been inactive for a pre-established duration. Automatic locking thresholds can be established at either the facility or user level, with the latter overriding the former. Facility locking thresholds are designated in minutes through the LOCKTIME suboption of the FACILITY control option, while user thresholds are set via the LTIME parameter of the TSS ADDTO command. LTIME takes precedence over LOCKTIME.

A virtual machine is considered inactive and subject to LTIME/LOCKTIME, when no CPU (as reported by TOTCPU in CP QUERY TIME) is being consumed by the virtual machine, either for virtual processing or for CP command execution. Disconnected terminal sessions are not subject to LTIME/LOCKTIME.

OS/DOS Data Sets and Volumes

To protect individual data sets on OS- or DOS-formatted volumes, you must elect to install either CP-level or CMS-level Data Set Protection. This is accomplished by selecting specific options during product installation. These options may also be added at a later time by reopening certain installation tasks. Complete information on required procedures may be found in the *Getting* Started.

There is no default or minimal data set protection mechanism; if Data Set Protection is not specified, these resources are protected only at the minidisk access level.

The two types of protection--CP and CMS--differ in mode of operation, implementation method, and functional characteristics. Choosing between two (or choosing to use both) requires consideration of various factors including the types of applications running on your system, the type of users, and your DASD configuration.

CP-level Data Set Protection

The CP-level Data Set Protection option is selected prior to updating the CP nucleus and results in the inclusion of additional CA Top Secret modules into the VM control program. Its function is to intercept actual I/O operations on DASD devices initiated by guest virtual machines. CP-level Data Set Protection does not rely on any guest interface, data set open processing routines, or additional code in the user's address space, nor does it require the use of any specific guest operating system. It functions properly regardless of the method used by the virtual machine to perform the I/O operation, since it identifies the target data set of the operation by examination of the actual channel program before it reaches the hardware.

CMS-level Data Set Protection

The CMS-level Data Set Protection option is installed in the CMS nucleus as directed by an optional task which is invoked after CP and the server have been built. CMS-level protection functions in a more traditional way by providing security calls during normal data set open processing in CMS's DOS and OS simulation routines. If CA Top Secret fails the request, the open is not completed, and the user's program is not able to read or write records to the file.

Because of the design of VM and CMS, however, it is not always necessary to use the simulation routines to access a data set. A more experienced user may, for example, write a program to perform physical I/O (PIOCS) to the device and access the desired information without going through normal system access methods. If, on the other hand, your users are locked into protected applications, this method may be more appropriate. Consider these points, as well as the sensitivity of the data involved, in your selection. If you need absolute data security, you may want to choose CP-level Data Set Protection.

Comparison of CP-level Versus CMS-level

These two DASD data security methods differ in behavior and in the data configurations they support. The following table summarizes these differences:

CP-level	CMS-level
All VSAM I/O treated as SYSVSAM.Vvolser	Supports VSAM by cluster/catalog name
Enforced only for full-pack minidisks	OS- or DOS-formatted minidisk support
Intercepts actual I/O,guest operating system-independent	Enforced only for programs using CMS OPEN interface
May be disabled system-wide with NOSIOCHK control option	Always active if installed in the IPLed CMS system

CP-level	CMS-level
Cannot be bypassed	Can be defeated by sophisticated users
Fails access on first physical I/O to data set with condition code 3	Fails access at OPEN time

Another important consideration in evaluating CP-level Data Set Protection is that it may deny access to certain unusually complex channel programs whose design prevents, or presents a threat to, accurate data set identification. While such channel programs typically indicate a deliberate attempt to circumvent security, it is possible for a well-intended program or system to unintentionally encounter this situation if it is using unusual I/O techniques or accessing nonstandard direct-access data structures. This denial occurs for undefined or DORMant users. You must identify users of applications with the potential for risk in this area and test this feature with them before implementing it.

Also be aware that neither of these two types of protection are intended to be used with other guest operating systems or with multi-user service virtual machines (such as data base servers). Since these systems perform work on behalf of a number of different accessors, CA Top Secret is unable to determine whose authority to apply for access verification. Such systems must provide their security or request verification on behalf of end-users via the CA Top Secret Application Interface, and must be defined with NOVOLCHK and NODSNCHK attributes.

See the *Implementation Guide* for additional information on data set security implementation procedures.

SFS Command and Directory Protection

CA Top Secret security for the IBM Shared File System (SFS) environment utilizes the CA-CIS CA-ESM component. CA-ESM “tells” the SFS server machine that external security is in effect. All user requests to access SFS directories and files, as well as some SFS command requests, will then be redirected to the CA Top Secret server machine. The DIRECTRY and SFSCMD resource class keywords can then be used to customize ACID access to these resources. The purpose and syntax example for both resource classes follow this section.

For further information on the CA-ESM component, refer to your CA-CIS documentation.

Protecting SFS Directories

The DIRECTRY resource class is used to retrict user access to particular SFS directories. The syntax is as follows:

```
TSS PER(acid) DIRECTRY(directory[ .subdirectory,],...)

    [ FILE(filename) ] \{ POOL(filepool) \}

                       \{ ACCESS(level)\}
```

Note that if you have stored commonly used or accessed EXECs or files on an SFS directory, you should PERMIT that directory to the ALL Record with an access level of READ.

For further information on the DIRECTRY resource class, refer to the *Implementation* and *Command Functions* guides.

Protecting SFS Commands

The SFSCMD resource class is used to restrict ACID access to certain SFS commands. The syntax is as follows:

```
TSS PER(acid) SFSCMD(cmd [ .filepool ],...)
```

Chapter 14: Logging and Reporting Options

This section contains the following topics:

Logging Activity and Violations (see page 77)
Reporting Activity and Violations (see page 77)
Logging and Violation Control Options (see page 79)

Logging Activity and Violations

One of the main functions of a security product is to control unauthorized access attempts by users in your data processing environment. An equally important function is to track security violations and other selected activity.

CA Top Secret provides you with an Audit File to record security violations. As with the Security, Backup, and Recovery Files, the Audit File can be shared with an MVS or VSE system.

Audit File

There are certain advantages to using the Audit File:

- Logging to the Audit File cannot be turned off. This eliminates a potential security exposure.
- Reports can be generated for “up to the minute” information.
- TSSUTIL can be used to routinely archive Audit information.

Select Type of Activity for Logging

You must select the activity you wish to log. This can be done globally or by facility through the LOG control option or the LOG suboption of the FACILITY control option. Violation activity is always logged as long as you have included the Audit File in the CA Top Secret start-up procedure.

Reporting Activity and Violations

One of the easier ways to monitor violations, or any selected activity, is to develop and produce reports on a regular basis. TSSUTIL, CA Top Secret’s report generator, allows you to produce violation and/or activity reports based on customized selection criteria. The *Reporting Guide* discusses the use of TSSUTIL.

TSSCFILE

TSSCFILE is a batch utility that produces a fixed format output file whose records closely parallel the output of the TSS LIST command function. A six-character identifier is associated with each record type. Scope and administrative authority limitations are honored. This file can be used for writing customized reports. For example, the output of TSSCFILE can readily become the input for CA-EARL, the comprehensive report writer from Computer Associates.

TSSREPT

TSSREPT applies the capabilities of CA-EARL to the output of TSSCFILE or TSSUTIL in order to provide formatted summaries of CA Top Secret data. With the appropriate CA Top Secret administrative required authority, this expanded reporting function gives you the capability to generate additional administrative summary reports.

TSSAUDIT

TSSAUDIT allows the auditor to monitor changes to the CA Top Secret Security File. This batch utility program lists Security File information about all ACIDs and their attributes and privileges.

Generating Reports

When generating reports, it is a good idea to segment the information that you are monitoring rather than to produce one large report for your organization. If you segment the critical selection criteria from the non-critical, you can more easily focus on critical information.

Consider the following sample breakdown of daily reports:

- Report A contains violation information against all data sets.
- Report B contains violation information against each data set and indicates which ACID requested access, what type of access was requested and what access level was allowed for that ACID.
- Report C contains information about all ACIDs that have received password violations.
- Report D contains initiation information for all terminal violations.

While the needs of each organization differ, you can see that when reporting is segmented such as in the sample breakdown, it is much easier for the Security Administrator to review critical violations and activity because the critical information is structured in such a way that it stands out from the less critical information.

Ad Hoc Reporting

You can also produce ad hoc reports that address special situations. For example, if you suspect that one of your users has suspicious access patterns, you might audit the user and produce a one-time report of the activity.

User Message and Violation Suppression

You can choose to suppress sending messages to users in WARN mode by not specifying the MSG suboption of the LOG options. You can suppress sending selected messages to users through the MSG control option.

You can also suppress selected violations issued to users, but not the logging of violations, by changing characteristics of detailed violation reason codes through the DRC control option.

Avoid Message Suppression

Suppressing messages may be an acceptable implementation strategy particularly during the testing stages. It is recommended, however, that you avoid message or violation suppression if possible. User messages and violations are often an important debugging tool when you are trying to resolve user problems. If you find that you must suppress messages, you may cautiously choose the messages or violations that you are going to suppress. Communicate to any person who handles security problems that users may not be receiving the selected messages or violations.

Logging and Violation Control Options

The following control options affect CA Top Secret's logging and message generation routines:

DRC

The DRC control option allows you to tailor the behavior of CA Top Secret by the Detailed Violation Reason Code. This allows you to customize the way selected violations are handled within your organization.

This option, by design, cannot suppress the logging of violations to the Audit File.

LOG

The LOG control option and the LOG suboption of the FACILITY control option, control the logging of information to the CA Top Secret Audit File. These options allow you to specify the selected activity that you wish to log.

No matter which options are specified, violations and audited events are always logged as long as you have specified recording media.

MSG

This option allows you to modify message characteristics for your installation. You can alter the way in which the message is issued, but you cannot alter the text of the message with this option.

VTHRESH

This option sets a violation threshold for non-password related violations which when exceeded takes a selected action against the user. The threshold count is refreshed for each session. The actions available include warning the user, cancelling the session and suspending the ACID. If you choose to suspend ACIDs, take care not to set the threshold too low to cause excessive suspensions from accidental unauthorized access attempts.

Chapter 15: Define Procedures for Handling Violations

This section contains the following topics:

Monitoring Discourages Violation Attempts (see page 81)
Elements of Procedure (see page 81)
Conclusion (see page 82)

Monitoring Discourages 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 may indicate that these users are looking for a loophole in your security definitions. If they find the loophole, this **does not** show up as a violation. Therefore, a pattern of attempts might indicate a potential breach of security and they must 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 know they do not have access to.

Elements of Procedure

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

Consider the following procedure for handling excessive violations:

- Carefully monitor your regular violation reports to determine patterns of excessive violations by specific users or groups of users.
- If you identify suspicious users or groups of users, you might consider doing further research on access patterns by auditing the suspected ACIDs.
- Use TSSUTIL to produce regular reports on these users showing violations and all audited activity.
- 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.

- If you feel that these patterns must 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 can meet with the user to determine the cause of the access activity.
- If the panel decides that the cause of the activity is malicious or destructive in nature, a formal warning must 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 can continue to monitor the user's activity. If the excessive violation pattern continues, you are prepared to take action against the user, possibly dismissal. Management must, of course, support this type of action.

Conclusion

Your procedure for handling violations must be tailored to your organization, and 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.

A procedure such as the one discussed might sound severe. However, with such a procedure in place, employees become quickly aware of how seriously your organization is facing security issues.

You might not discourage the disgruntled employee or the dedicated internal hacker, but you can discourage the casual inquisitive employee. Even if you do not discourage disgruntled employees and hackers, you are least prepared to take disciplinary action and enforce the security that you are taking so much time to implement.

Chapter 16: Plan Emergency and Troubleshooting Procedures

This section contains the following topics:

Production Security Violations (see page 83)
CA Top Secret Software Problems (see page 83)
Disaster Recovery (see page 84)

Production Security Violations

Production abends caused by security violations can occur at any time and when least expected. They can occur if someone has revised a procedure without requesting the appropriate CA Top Secret definition revisions, or if an untested change to a CA Top Secret definition has been made. In any event, the appropriate authority must be available at all times to make the production piece operational.

If production problems occur during working hours, the security administration staff must be prepared to respond to emergency production problems so as to not impact the production schedule. At least one member of the security administration staff must be available at all times to analyze and resolve the problem as quickly as possible.

For production problems occurring after normal working hours, special “emergency” ACIDs can be defined. These User ACIDs are permitted extensive access to production resources but must be audited. Administrative procedures must be set up to tightly control the use of these ACIDs. Considerations include who are given access to the passwords, how often they are changed, and who is responsible for reviewing audit reports, etc.

CA Top Secret Software Problems

One important characteristic of CA Top Secret is that as a Security System it is by nature a critical part of your operating environment. CA Top Secret is designed to recover from virtually any system error or abend. However, loss of CA Top Secret’s files, or major operating system errors may cause system failure. Almost exclusively, errors that cause CA Top Secret unrecoverable problems are in the area of file destruction, and for this reason recovery procedures, as discussed in the “Backup and Recovery Procedures” chapter must be an integral part of your security and operating system plan.

Another important element is the fact that CA Top Secret, by its nature as a security system, makes every effort to protect itself from attack, and, if necessary, disables the operating system before allowing unauthorized security bypasses to occur.

If, for any reason, known or unknown, CA Top Secret behaves in an unexpected manner, you can be prepared to solve and circumvent system problems in an emergency situation. The following points may be useful in an emergency situation:

- CA Top Secret has secure means of bypassing selected parts, or the entire security system. Be familiar with them and test their operation occasionally.
- CA Top Secret recovers virtually all internal errors. Be sure that procedures exist for printing snap dumps taken by CA Top Secret and delivering this information to the proper systems areas in a timely fashion.
- Most problems with CA Top Secret involve security authorizations not working in the manner expected. Use CA Top Secret diagnostic tools when contacting CA Top Secret Customer Support. If the preparation for problem diagnosis is proceduralized, this results in faster, more accurate resolutions from CA when needed.
- If CA Top Secret has completely failed, a system IPL without CA Top Secret may be in order. IPL processes to accomplish this can be set up, but must only be known to a select group of trusted employees. If there is more than one CPU in your complex, this may be unnecessary if the unaffected CPU can be used to address the problem.
- Since any problem may occur off hours, contact lists and phone numbers of your security personnel and for Computer Associates emergency support must be available. All responsibilities must be clearly understood by all participants.

Disaster Recovery

Disaster recovery plans are usually fairly involved and complex. It is a huge task to move an entire data center to a new location under emergency conditions. When you begin to implement CA Top Secret, your disaster recovery plan can be modified to include procedures to bring CA Top Secret to the disaster recovery site.

If Installing Operating System at Site

If your disaster recovery site permits you to install your version of the operating system, be sure to plan to bring the CA Top Secret server machine's minidisks to the site. CA Top Secret must be brought up after IPL, just as it is at your main site.

If Using the Site's Operating System

If the site provides you with an operational operating system, be sure that you can install CA Top Secret at that site as part of your disaster recovery operation. Since CA Top Secret installs quickly, your disaster recovery procedures are not impacted by the installation of your security software.

Plan to Install Security

No matter which type of disaster recovery site you are using, you can plan to include the installation and use of CA Top Secret as part of disaster recovery testing. The time of a disaster is not the time to try to bring CA Top Secret along for the first time.

Some organizations choose to leave security products out of disaster recovery plans. They feel that in a disaster, they do not have to worry about security. This of course leaves the data center exposed. Also, knowledge of this omission might encourage sabotage against your main data center to force you to relocate to an unsecured operation.

It is strongly recommended that you plan to install CA Top Secret at your disaster recovery site to protect your operation even in an emergency situation.

Chapter 17: Define Audit Requirements

This section contains the following topics:

Audit Requirements (see page 87)
Defining CA Top Secret Auditors (see page 87)
Defined as Administrators (see page 87)
Using CA Top Secret Auditing Capabilities (see page 88)
CA Top Secret Utilities (see page 88)
Auditing Users and Resources (see page 89)

Audit Requirements

Your internal auditors can monitor the effectiveness of the security implementation and adherence to any policies that have been defined. In most organizations, the EDP auditors perform this function. Their responsibilities toward the security effort must be clearly defined in the security policy.

CA Top Secret has been designed with a number of auditing capabilities which allow auditors to audit the implementation and effectiveness of CA Top Secret. This chapter explains how best to put these capabilities to work.

Defining CA Top Secret Auditors

The auditors can be defined to CA Top Secret early in the implementation so that they can work with, and monitor activity of the security administration staff. If the security administration staff and the auditors work together throughout the implementation, each strategy can be evaluated before it is implemented. This can save implementation time and potential rework.

Defined as Administrators

CA Top Secret auditors are defined to CA Top Secret as Security Administrators and can be defined at any level. You may choose to define a central level auditor (SCA) or limited central level auditor (LSCA) as a permanent account to perform routine security audits. Zonal (ZCA), Divisional (VCA) and departmental (DCA) auditors are often temporary accounts defined to allow periodic audits of corporate functional areas.

As with any CA Top Secret administrator, you must assign the proper auditing authorities to the audit accounts. Typically, auditors are allowed to list information from the CA Top Secret Security File and use the CA Top Secret auditing tools.

See the *General Concepts Guide* for information on how to define CA Top Secret auditors.

Using CA Top Secret Auditing Capabilities

The CA Top Secret auditing tools are available to any administrator defined with auditing authorities. The security administration staff might use these tools to monitor and to help control their activity.

The following commands are available tools for reviewing the CA Top Secret Security File:

- TSS LIST
- WHOOWNS
- WHOHAS

These commands allow the auditor to review the Security File for information on specific ACIDs or resources.

CA Top Secret Utilities

This section describes the CA Top Secret Utilities.

TSSUTIL

TSSUTIL is used to monitor violations and other activity including audited activity. This utility is discussed briefly in the "Logging and Reporting Options" chapter.

TSSAUDIT

TSSAUDIT is used to monitor changes made to the Security File. This utility is also discussed briefly in the "Logging and Reporting Options" chapter.

TSSCFILE

TSSCFILE is used to extract TSS LIST, WHOHAS, and WHOOWNS information into a flat file for further processing by a report generator, such as CA-EARL.

Auditing Users and Resources

An CA Top Secret auditor has the authority to audit users and resources. To audit users, the auditor attaches the AUDIT attribute to the user's ACID. To audit resources, the auditor updates the AUDIT record with the resource or resource prefix to be audited.

The auditor may wish to audit critical resources on a permanent basis and produce reports or monitor online the results of the audit. The auditor may also wish to spot-check user activity by periodically auditing key personnel.

The auditor may wish to coordinate the audit activity with the Security Administrator. The Security Administrator may do concurrent audits to monitor effectiveness of the security implementation.

Note: Carefully select audit criteria, and revise this criteria as audit requirements change. This avoids the unnecessary generation of large numbers of audit records.

Chapter 18: Define Security Maintenance Procedures

This section contains the following topics:

Security File Maintenance (see page 91)
Verifying Change Requests (see page 91)
CA Top Secret Software Maintenance (see page 92)

Security File Maintenance

Ongoing maintenance must be an important concern during and after the security implementation. This maintenance can 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 in anticipation of the first request.

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

As your environment changes, as is common in most installations, you are 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 can have a CA Top Secret Security File maintenance procedure which allows you to ensure that the requested revisions are correct and authorized.

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 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 which owns the resource(s) be responsible for verifying the necessity and accuracy of change requests. The request must be made in writing with the proper authorization.

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 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.

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.

Design Procedure For Quick Turnaround

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

The ability of a central security administration staff to respond quickly to maintenance requests may 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.

CA Top Secret Software Maintenance

CA Top Secret software maintenance is usually delivered twice a year. You may receive your first Service Pack Tape before your implementation is completed. Therefore, you must be prepared to apply this maintenance during the early stages of the implementation process. This ensures that your site can run CA Top Secret software up to its current level of maintenance.

Reason for Software Maintenance

Usually CA Top Secret maintenance is required to introduce new or enhanced security product features into the environment. In this case, an organization can take their time in installing the maintenance.

On occasion, however, CA Top Secret maintenance is provided to fix system problems. This type of maintenance might be delivered on the twice a year Service Pack Tape, or you might receive this maintenance from CA Top Secret Customer Support in response to a specific problem that your organization is experiencing. An emergency security product maintenance procedure must be available to respond to this type of situation, particularly if your organization is being impacted by these system problems.

Software Maintenance Considerations

A number of considerations should be taken into account when doing CA Top Secret maintenance:

- The maintenance must be scheduled at a time when it has the least impact on your environment.
- Test plans must be available to ensure that CA Top Secret is still functioning as designed for your environment.
- DO NOT update the CA Top Secret object code with your in-house modifications. This negates the integrity of the CA Top Secret software. CA Top Secret anti-tampering code is in place to detect unauthorized modifications to CA Top Secret software and CA Top Secret disables the operating system or forces reinitialization of an unmodified CA Top Secret if this occurs.

System Software Maintenance

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

VM Access Control Interface

CA Top Secret accepts and validates all security-checking requests issued by the security calls inherent in VM's access control interface. It also establishes additional interfaces when the standard access control interface is deficient. This is dependent upon the stability of the access control interface and of the existence of certain CP modules. When upgrading your VM system to a new release, it is recommended that you contact your CA Top Secret representative to ensure that your maintenance level of CA Top Secret is compatible with the new VM system.

Chapter 19: Develop Testing Procedures

As with any piece of 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. All checks are done out of the access control interface that is part of the VM operating system.

Chapter 20: Customization

This section contains the following topics:

Common Reasons for Customization (see page 97)

Common Reasons for 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.

Customization is most often with:

- Virtual Machine Interfaces
- The CA Top Secret Installation Exit

Virtual Machine Interfaces

CA Top Secret has an interface through which application programs and guest systems can request specific security services. This interface is described in the Customization Guide.

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 sync across CPUs

- Provide interfaces for second level authentication devices
- Log additional information 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.

Conclusion

Avoid customization through any other means than that detailed above. Computer Associates is committed to support only the CA Top Secret capabilities.

Many CA Top Secret customers have successfully customized their use of CA Top Secret through the available capabilities. 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 eliminates a customization requirement.

Chapter 21: Develop Security Awareness Programs

This section contains the following topics:

[About Security Awareness Programs](#) (see page 99)
[Goals of Awareness Program](#) (see page 99)
[Cultivate Cooperation](#) (see page 100)
[Educate the Security System Users](#) (see page 103)

About Security Awareness Programs

Each implementation is unique because there are so many variables involved. But the most significant variable is that people are involved and that security becomes an emotional and political subject. People might feel threatened by the advent of security in your organization. They might feel that it interferes 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 results in acceptance and support of the security program in your organization.

Goals of Awareness Program

The major goals of a security awareness program are to:

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

Cultivate Cooperation

It is more effective if individuals in your organization monitor the security program in their 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. Each area is discussed in relation to why they may be opposed to security, why their cooperation must be cultivated, and how that cooperation may be cultivated.

Systems Software Area

These individuals are usually 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 aware of more different and creative ways to access those resources than any other area in the shop, and they may have 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 gets in the way of doing their job.

Cooperation must be cultivated in this area for two important reasons. First of all, CA Top Secret software maintenance is the responsibility of this area. In order to effect smooth maintenance procedures, a cooperative spirit must 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 can 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 so that system resources are protected and only authorized accounts are allowed to access them at specific access levels for required functions, such as VM maintenance. It is important to note that these resources are no longer available to anyone other than the system software area. They may continue to be available within the software area, but only at the needed access level so that system resources are not accidentally damaged.

As long as the system software personnel are not continually at cross-purposes with CA Top Secret while trying to do the job, they 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.

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 which comprise their application and some globally accessible system resources. Initially, there may be a fear of CA Top Secret. The classically curious applications people, who like to roam unbridled through system resources, feel threatened that their curiosity is being thwarted. But these individuals are usually the exception, and must not be nosing around as part of their job function.

Actually, these areas may welcome CA Top Secret if they are properly educated in its use. CA Top Secret provides an applications interface which 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 requires different security definitions so protecting this area may be a slow process. Each application design must be evaluated for effective protection, and the security administrator is well advised to involve the affected application area in the security definition process.

Operations

The operations staff has a very important but harrowing task to perform. They have to get production processing completed on time but contend 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 production being completed. But you must take the time to cultivate the cooperation of the operations area in supporting CA Top Secret or else 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 which allow them to get production through with minimal delay as discussed in the “Plan Emergency and Troubleshooting Procedures” chapter.

Although the operations staff is usually the least involved with the implementation plan for CA Top Secret, they can be the most seriously impacted by it. Careful consideration must be made to ensure that production runs 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.

The Auditors

The auditing area is usually the only area that enthusiastically supports the CA Top Secret implementation since it is the responsiblity of the auditors, 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 don't 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 are not in a position to criticize and force rework of strategies at a later time because their direct input was 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 must be developed early in the security design phase to allow the auditors to monitor activity as the implementation progresses. This is discussed in the "Define Audit Requirements" chapter. Auditors may be able to offer input on design requirements as a result of this review, and this may prove significant in tightening the security procedures developed.

Applications End-Users

This group is usually 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 usually the most knowledgeable, however, in how the resources used in their areas are accessed, and by whom. They are also a good source in determining the criticality of information 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 is invisible internally. In fact, their greatest exposure to the need for security 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 support the use of security but not if it becomes something that prevents them from simply doing their job. Therefore, security definitions for this group must be handled 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 one of 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 simplifies the security centralization effort.

If you take the time to ensure that you have taken into account the psychological needs of each area, as well as the technical requirements, your implementation proceeds more smoothly than you might expect. In fact, you may find that you are receiving assistance and support from all of these areas. This is an important step toward achieving truly effective security in your environment.

Educate the Security System Users

Someone once said that "...people fear that which they do not know." This adage definitely applies to the area of security. 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 are designed in such a way as to provide information to the users concerning new security features and facilities. Also, education must be made available when new users come into your organization.

Subject Matter

Some of the subjects which can be addressed and the intended audiences are as follows:

- For systems software personnel: CA Top Secret installation and information on how CA Top Secret interfaces with the operating system.
- For systems software and applications 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 area requiring the ability to audit: information on how to use CA Top Secret to monitor the data processing environment without impacting the operation of the shop.

  For all users, information on ACID and password requirements includes the following:

  - How often the password is changed, and the procedure which must be followed to revise it.
  - Under what circumstances an ACID may be suspended, and what to do about it.

- For all users: what kind of violation messages they may encounter, and what action is required for each.
- For all users: 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.

Training Development

Individual training programs can be developed for each functional area, or training can be organized by subject. The training must 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.

Communicate the Security Policy

In order 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: Global distribution of the physical document to all users. The document can be included with your organization's personnel policies and procedures manual.
- Formal Presentations: Formal presentation of security objectives to all users. This can be included with CA Top Secret training.
- Performance Review Checklist: Inclusion of 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 that are available for purchase or rental for these seminars. You can contact your CA Top Secret user groups or security organizations for information on these films.

Chapter 22: Schedule Ongoing Evaluation

This section contains the following topics:

Ongoing Evaluation (see page 107)
Evaluation Team (see page 107)
Team Responsibilities (see page 107)
Annual Security Review (see page 108)

Ongoing Evaluation

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

Evaluation Team

You might establish a security evaluation team--even during the implementation--that might be comprised of the members of the initial project team. Minimally, the team can 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 can 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 become a part of any environmental change once your organization is committed to implementing a security product. These considerations 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.

Annual Security Review

Although you can continually monitor your security environment, it is recommended that you plan an annual security review by qualified professionals.

Appendix A: Sample Security Policy and Maintenance Form

Human Resource Security Policy

SUBJECT	Human Resource Security Policy
EFFECTIVE	For all Zones on July 1, 2008
OBJECTIVE	To ensure that human resources is protected from accidental or intentional unauthorized modification, destruction or disclosure.
ISSUING OFFICERS	Vice President - Personnel
	_____
	Authorizing Signature
	Vice President - Personnel/Operations
	Vice President - Administrative Planning
	Vice President - Internal Audit
	Vice President and Treasurer - Financial Control
CROSS REFERENCES	None

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.

POLICY

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, such as source code, job control, and load modules, because these are the means through which the data can be accessed, altered or destroyed.

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 centrally processes all maintenance to human resource data.

3. Access Responsibility

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

4. 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.

5. Procedure

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

6. 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.

   - 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 that 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.
   - 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 secure 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 in order 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.
   - 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 secure manner to appropriate field personnel or other approved recipients.
     - To secure the Payroll area in order 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.

- 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.
  - Distribute reports and other savings plan information in a secure manner to appropriate field personnel or other approved recipients.
  - To secure the Benefit Plans Accounting area in order to maintain the confidentiality of all employee information under their control.
- 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.
- 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. 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 is 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.

- 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 in order to restrict access to automated procedures and facilities.
- 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 in order to maintain confidentiality of human resource information while it is under their control.
- 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.

Sample Maintenance Form

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:

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