TANDEM

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 2, Release 2

4 March 2005

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

APPENDICES

SUMMARY OF CHANGES

Changes in this document since the previous release (Version 2, Release 1, dated 9 June 2003) are listed below.

GENERAL

Updated cover page, headers, and footers with the newest version of the Section 1 template.

SECTION 1. INTRODUCTION

Made changes based on STIG consistency efforts.

This page is intentionally left blank.

1. INTRODUCTION

In today's world, personnel at every level and echelon need information in order to perform their jobs. The Department of Defense's (DOD’s) reliance on networked information has increased dramatically. Information drives the decision-making process, and accurate and timely information is essential for making decisions. This increased reliance requires that the information be available when needed, that the storage and transport process assures the integrity of the information, and that the information be available only to authorized users. Since information that the warfighter depends upon can be stored, processed, or transmitted from a number of locations, information systems management and Information Security (INFOSEC) must contend with the total environment.

Technology can provide so much information that efficient management, sorting, manipulating, processing, storing, and transmission have become major elements in providing the proper information to users of the entire Global Information Grid (GIG). Relevant information can be so disbursed that reliance on a single information source may be inadequate. As the DOD systems and networks become more interrelated and sophisticated, ensuring the security of this information has become even more complex.

Security in this interactive operating environment must focus on the entire GIG and not simply on individual systems and networks. In addition to securing information while in transit across the GIG, a major effort must be placed on ensuring that networks attached to the GIG do not present a security problem to other users within the GIG. This concern is heightened by the fact that network vulnerabilities become magnified when external access is permitted. The GIG is only as secure as its weakest component and threats can be global as well as local. However, a secure backbone network is necessary to minimize the risks for the attached connections while ensuring the required interconnectivity.

The intent of this *Tandem Security Technical Implementation Guide (STIG)* is to include security considerations needed to provide an acceptable level of risk for the information that resides on the Tandem systems.

It should be noted that FSO support for the STIGs, Checklists, and Tools is only available to DOD Customers.

1.1 Background

Department of Defense Directive (DoDD) 8500.1 establishes policy and assigns responsibilities to the Defense Information Systems Agency (DISA) to develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with the National Security Agency. Paragraph 4.18 of the 8500.1 states, " All IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines." DISA Field Security Operations (FSO) develops the guidelines, which are called Security Technical Implementation Guides.

Attacks on DOD computer systems are a serious and growing threat. The number of attacks is doubling each year, as Internet usage increases along with the sophistication of hackers[1] and their tools.

At a minimum, these attacks are a multi-million dollar nuisance to the DOD. At worst, they are a serious threat to national security. Attackers have done the following:

- Seized control of DOD systems, many of which support critical functions such as weapons systems research and development, logistics, finance, procurement, personnel management, military health, and payroll.

- Systems and networks, denying service to users that depend on automated systems to help meet critical missions.

- Stolen, modified, and destroyed data and software.

- Installed unwanted files and back doors that circumvent normal system protection and allow unauthorized access in the future.

In preventing computer attacks, the DOD must protect a vast and complex information infrastructure. Currently, it has over 2.1 million computers, 10,000 local networks, and 100 long-distance networks. The DOD also depends critically on information technology. It uses computers to help design weapons, identify and track enemy targets, pay soldiers, mobilize reservists, and manage supplies.

The DOD is relying on the Internet to enhance communication and information sharing. In turning to the Internet, DOD has increased its own exposure to attacks. More and more computer users (currently over 40 million worldwide) are connecting to the Internet. Internet connections make it possible for enemies armed with less equipment and weapons to gain a competitive edge at a small price. As a result, this will become an increasingly attractive way for terrorists or adversaries to wage Information Warfare (INFOWAR) attacks against DOD.

The National Security Agency (NSA) acknowledges that potential adversaries are developing

[1] The term, **hacker**, has a relatively long history. Hackers were at one time persons who explored the inner workings of computer systems to expand their capabilities, as opposed to those who simply used computer systems. Today the term generally refers to unauthorized individuals who attempt to penetrate information systems; browse, steal, or modify data; deny access or service to others; or cause damage or harm in some other way.

methods to attack DOD and other U.S. systems. According to DOD officials, these methods (which include sophisticated computer viruses and automated routines) allow adversaries to launch untraceable attacks from anywhere in the world. In some extreme scenarios, studies show that terrorists or other adversaries could seize control of DOD information systems and seriously degrade the nation's ability to deploy and sustain military forces. Official estimates show that more than 120 countries already have, or are developing, such computer attack capabilities.

In guarding its information, DOD faces the same risks and challenges as other Government and private sector organizations that rely heavily on information technology. The task of preventing users (both authorized and unauthorized) from compromising the confidentiality, integrity, or availability of sensitive information is increasingly difficult and resource intensive in the face of the growth in Internet use, the increasing skill levels of attackers, and technological advances in their tools and methods of attack.

1.2 Authority

DOD Directive 8500.1 requires that “all IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines” and tasks DISA to “develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.” This document is provided under the authority of DOD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the MAC II Sensitive level, containing sensitive information.

1.3 Scope

This *Tandem STIG* covers the operating system(s) (OS), applications, and security tools displayed in the following table:

OS	***TANDEM NONSTOP KERNEL***
Access Methods	Tandem NonStop SQL (NSSQL) Tandem Enscribe
Security Tools	Block Mode Operating System Services (BOSS) Command Interpreter Monitor (CMON)

The requirements set forth in this document will assist IAOs and IAMs in securing the Tandem NonStop Kernel operating system (OS) for each site. The Tandem OS, (referred to hereinafter as Kernel) includes the Tandem NonStop SQL [NSSQL] database management system (DBMS), and the Tandem file management system Enscribe. The document will also assist in identifying external security exposures created when the site is connected to at least one IS outside the site's control. The site's Configuration Control Board (CCB) will approve all major revisions to site systems. Therefore, before implementing Tandem security measures, the IAO or TASO should submit a change notice to the CCB for review and approval. If CCBs (other than the site's CCB) are involved in making major system revisions, the IAO or a representative should also be attending these other CCB meetings.

DISA has a group responsible for Tandem system-wide software support (design, development, testing, and maintenance functions for the system-level utilities) called the Systems Support Office (SSO). For clarification in this document, the designated representative from the staff that performs this function will hereinafter be referred to as the SSO.

The Navy has a group responsible for Tandem applications software support (design, development, testing, and maintenance) called the Central Design Activity (CDA). The equivalent Air Force group designated to perform the CDA function is called the Material Systems Group (MSG). For clarification in this document, the designated representative, from the staff, that performs this function will hereinafter be referred to as the CDA. CDAs should address security requirements as part of their application development and lifecycle management process. Additionally, the DOD Information Technology Security Certification and Accreditation Process (DITSCAP) addresses security as part of an application's accreditation process. CDAs should have a security person providing guidance to any Configuration Control Board (CCB) meetings concerning Tandem applications or functional code releases. The DISA Application Security Working Group (ASWG) is developing a set of security documents for use by application developers. The first document, *Recommended Standard Application Security Requirements,* is available on the Guides and IASE web sites (see *Section 1.6, STIG Distribution*). The *Application Security Developer's Guide (Draft)* is a "How To" guide based on the Recommended Standard Application Security Requirements document and is currently available. The group of documents is herein referred to as the FSO Security Review Methodology. The group is also researching assessment tools that could be used by developers in a test environment. The result of a market survey conducted on vulnerability assessment tools is also available. Any questions about applications development security controls should be directed to DISA Field Security Operations.

The local site, where the Tandem resides, is ultimately responsible for the Tandem security. The local site Commander/Director must be fully aware of all the risks on the Tandem (to include those that may be created by having certain applications on the Tandem). These risks may be required for certain INFOCON levels and might affect subsequent operational issues. For this reason, each local site will be the primary party responsible for fixing any SRR (Security Readiness Review) findings. Agreements that address security requirements for applications, operating systems, and networking will be maintained at the local site, and these agreements must be in accordance with the *DISA Computing Services Security Handbook*.

- *The IAO at the local site is responsible for maintaining agreements (related to security requirements documenting the roles and responsibilities) and will provide assurance that all applications, operating systems, and networking security requirements are covered.*

1.4 Writing Conventions

Throughout this document, statements are written using words such as “**will**” and “**should**.” The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses “**will**,” indicate mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This makes all “**will**” statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to “**should**” indicates a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows "(*G111: CAT II*). "If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "*[N/A: CAT III]*").

1.5 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

Table 1.1. Vulnerability Severity Code Definitions

1.6 DISA Information Assurance Vulnerability Management (IAVM)

The DOD has mandated that all IAVMs are received and acted on by all commands, agencies, and organizations within the DOD. The IAVM process provides notification of these vulnerability alerts and requires that each of these organizations take appropriate actions in accordance with the issued alert. IAVM notifications can be accessed at the Joint Task Force - Global Network Operations (JTF-GNO) web site, http://www.cert.mil.

1.7 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is http://iase.disa.mil/.

1.8 Physical/Personnel Security

Although this document does not address physical or personnel security directly, these areas must be given proper consideration and attention. As an example in the case of network operations, it is widely documented how to gain privileged level access to Cisco routers with simply having physical access to the equipment and a laptop or other terminal devices. Proper attention to personnel security is necessary to ensure that only personnel with the proper credentials have access to the Tandem configuration.

- *The site’s security officer will ensure that the physical/personnel security requirements are adhered to, as contained in the DISA Computing Services Security Handbook, Section 3.1.5 (see Appendix C, Initial Tandem System Setup) and DOD 5200.1-R Information Security Program Regulation, 14 Jan 1997, & 5200.2-R Personnel Security Program, January 1987.*

- *The site’s security officer will ensure that the DISA Form 41 or similar access authorization form will be used to validate a user’s requirement to have at account on any Tandem.*

1.9 Education and Awareness Programs

For the system integrity, guidelines and policies to function, managers and employees in the Systems/Technical Support and Security offices must periodically be advised of their responsibilities regarding the protection of the Tandem systems.

The IAO, and other personnel to whom security administration functions have been delegated, will receive adequate and continuing training in the use and implementation of Kernel, $BOSS, $CMON, and other COTS/GOTS security products being used at the sites for which they are responsible.

Personnel in the Systems/Technical Support office will receive adequate training in the installation and maintenance of the Access Control Products (ACPs) in use at the sites for which they are responsible. They will also receive adequate and continuing training covering Kernel and COTS/GOTS security product functionality.

The DISA Certification Program Training Requirements for System Administrators (SAs) and Information Systems Service Providers (SSPs) provides guidance to accomplish the directives outlined in the memo subject, “Revised Certification Program Requirements for System Administrators” signed by the Chief of Staff, 29 November 1999. DISA requires that all SAs be certified, at a minimum, to Level I.

- *All Tandem SAs at the local site will be DISA Level I certified.*

1.9.1 User Awareness

User awareness involves keeping users updated and aware of vulnerabilities and performing regular risk assessment audits. By explaining the risks involved, the strategy being pursued, and the role each individual plays, Network Security Officers (NSOs), IAOs, and Terminal Area Security Officers (TASOs) encourage compliance and tolerance of any inconveniences imposed in accordance with the *DISA Computing Services Security Handbook, Section 11.*

- *Continued user and support staff awareness training and corrective action will be performed as determined by the IAO. Measures should include, but not be limited to, the following:*

    - *Detail each user’s responsibilities.*
    - *Provide written instructions on using data and client software outside the office.*
    - *Update users periodically on related policies.*

Examples of updated user awareness are as follows:

- Stay current on the latest virus information and signature updates by receiving e-mail from **viruslist@cert.mil** or visit the DOD-CERT web site at **www.cert.mil**.
- Stay current with the latest security concerns by receiving e-mail from **sans@sans.org**, or visit the SANS Institute web site at **www.sans.org**.
- Review the SA/SSP certification training CDs.

- Review security periodicals.

1.9.2 User Education

It is important that all users of Tandem information systems have a complete understanding of their responsibilities as users of the system and the related information stored on it. Users must understand the ramifications of not following proper procedures while using this equipment. Routine educational instruction will be provided in order to reinforce this knowledge. Policy and procedure updates will be provided in a timely manner to users.

- *The IAO will develop and distribute the Tandem Security Features Users Guide (SFUG) for the local site.*

2. TANDEM SITE OVERVIEW

2.1 Organizational Relationships

Organizational relationships play a significant role in providing for the security of the environment. The site organization must provide a robust and secure environment that protects the software environment from unauthorized access. This includes the protection of system-level resources (i.e., mainframe hardware, Kernel software, database systems, Pathway configurations, application subsystems, and other utilities used by the DOD user community/customers). Data owners must also play a role in determining access requirements for their resources (i.e., actual databases, master files, and interactive transactions). It is the responsibility of the data owners to provide an access matrix reflecting subjects (processes, data sets, applications, and other resources). Service Level Agreements (SLAs) will address security and define responsibilities of both the site and the customer.

2.2 Software Integrity

Tandem is an interactive, multitasking, and multi-user operating system. The Tandem operating system includes security that, with system security parameters set, in addition to the use of other security products, will meet C2 requirements. The C2 features are designed to meet the needs of the user environment and to meet the criteria defined in *DOD 8500.1-STD, Trusted Computer System Evaluation Criteria*.

This document provides requirements to limit the security vulnerabilities for a trusted system. These vulnerabilities and the steps required to mitigate them are discussed in this document. Commercial software vendors and developers, by providing software Vendor Integrity Statements (VISs) that guarantee the integrity and security of software they sell and develop, can guarantee software integrity. This is a requirement for all COTS (Commercial-Off-The-Shelf) products used by DISA. DISA Field Security Operations also attempts to guarantee software integrity through the DISA Code Analysis Team, which was created to analyze software that is not covered by VISs and to detect any security problems in the code. The Code Analysis Team works with code that is developed locally, free software available from the Internet, and GOTS (Government-Off-The-Shelf) products. DISA Field Security Operations works with vendors to obtain Vendor Integrity Statements for widely used software and operating systems.

- *The IAM will ensure that a Vendor Integrity Statement is requested within all software procurement actions for all commercial software products or a request has been made to Field Security Operations for verification of an existing Vendor Integrity Statement.*

- *The IAM will use, on all locally developed software or other GOTS software, the FSO Security Review Methodology or approved equivalent methodology and will retain the results of the review.*

- *When a Vendor Integrity Statement is not available for a software product, the product will be evaluated for vulnerabilities by one of the following groups:*

NOTE: Evaluated for Vulnerabilities occurs when software is reviewed, using the FSO's Security Review Methodology or approved equivalent methodology, to determine if there is any potential vulnerability in the software. Searching for potential vulnerabilities at the DOD-CERT, CERT/CC, SANS and in the X-Force DB and/or others places is also recommended on a routine bases.

  - *The site Configuration Control Board (CCB)*
  - *The site's local evaluation team utilizing FSO's Security Review Methodology or approved equivalent methodology*

- *For each site-unique developed and procured software product, the Vendor Integrity Statement field in the Software Contract Table of the Aperture Visual Information Manager database will be maintained to indicate the status of the Vendor Integrity Statement.*

- *Public domain software will not be used without the approval of the local configuration control board or evaluation using the FSO Security Review Methodology.*

2.2.1 Free Operating System Software

DISA requires that operating system software be obtained through a valid vendor channel and have a formal support path. Free Operating System software is defined as operating system source code or binary code that (1) is downloaded from the Internet, (2) has no clearly defined vendor channel, (3) has no clearly defined support path, and (4) has no chain of responsibility for updates and security notification. Some versions of UNIX and all versions of Linux fit this definition.

There are serious concerns about using this type of operating system (OS) software on a production network:

1. Software integrity cannot be guaranteed. There is no guarantee (such as a Vendor Integrity Statement) the code has not been modified in a malicious way.

2. DISA would require extensive source code analysis before using the code. Time and personnel are not currently available for this.

3. Vulnerabilities in the freeware code could be replicated to the entire network as soon as the system is connected to the network.

4. Freeware does not fully support the DISA requirements for operating systems, such as auditing.

5. Security patches are not readily available from reliable sources.

Any operating system being considered for use in a DISA production environment is subject to all of the requirements listed in *Section 2.2, Software Integrity,* and must be capable of STIG compliance as verified by an SRR.

These requirements conform to the spirit of the draft policy memorandum from the Assistant Secretary of Defense, *Guidance and Policy for Department of Defense Information Assurance, 24 June 1999*, *ASD (C3I)*. *Paragraph 4.11* states that all COTS and GOTS security-related software, hardware, and firmware will be evaluated prior to acquisition/implementation.

2.3 Security Administration

Currently, sites use both centralized and decentralized security administrations. Centralized security administration maintains authority and responsibility at one location. In this approach, access requirements are determined and documented, and are then forwarded to a centralized administrator. The centralized administrators reflect and maintain these requirements in the security environment.

Decentralized security administration maintains responsibility at one location but allows the selective delegation of authority to subordinate organizations. With this approach, the main administration of security remains at a central location. However, limited authority for administration capabilities can be delegated to an authorized person to maintain a subset of the security environment. Although the authority has been delegated, the ultimate responsibility remains with the central location.

The controls identified in this document are applicable regardless of the administrative approach currently being used.

2.4 Processing Environments

All Tandem IS sites use Kernel. As distributed by Tandem, Kernel provides integrity of the operating environment as part of the Trusted Computing Base (TCB), as defined in *DOD 8500.1-STD*. Controls have been developed and documented in Kernel references to ensure this integrity. Security mechanisms that maintain the integrity of the sites will be properly installed, configured, and maintained.

The target-processing environment as currently defined by Field Security Operations includes the Tandem Kernel, with CMON, and an implementation of the COTS Block-mode Operating System Services (BOSS) product to address the security need. The COTS BOSS product, CMON, and Kernel are to provide a standard security baseline for all sites by replacing the GOTS Security Access System (SAS) product at the Navy sites and addressing security needs for the Air Force sites. If Safeguard is installed at the site and it does not impede production processing, it is strongly recommended that Safeguard be used to aid in security management. Options specified during the installation, and techniques involved in the administration of these products, can increase or reduce the security assurance introduced into the individual operating environment. As a result, guidance is needed on how these products must be configured in the production operational environment.

Both open system and closed system environments are present at the sites. The main processing performed on site mainframes represents a traditional closed system approach to application processing. The newer and less controlled mid-tier platforms use the UNIX or Windows NT operating systems that traditionally represent open system environments. Even though they are considered a mid-tier platform, Tandem systems have the processing capacity of the mainframe and can function in either an open system or a closed system environment. Therefore, special consideration must be given to the security implications of both.

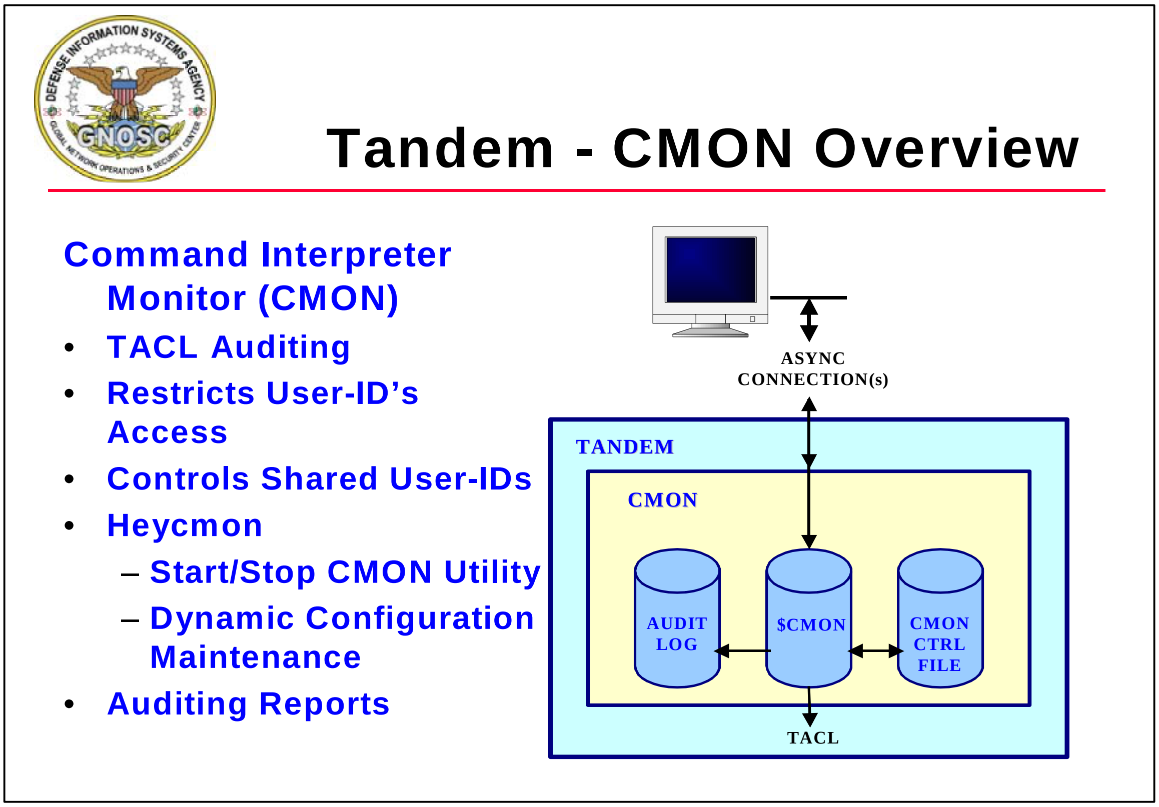
This page is intentionally left blank.

3. TANDEM SYSTEM SECURITY PRODUCTS

3.1 Kernel Access Security

Kernel controls operating system-level security with file system access controls and command-level userid access controls. Based on these two primary factors, Kernel allows or disallows functions to be performed. The administration of the Tandem system is performed through command-level SUPER group access. The system is configured, the database established, and the applications are installed using these two primary controls. This ensures that any process started or device/object accessed by a user has passed the verification process where the appropriate level of access authority had been previously granted by the IAO. The system can track all activities of the user with the unique identification in accordance with the *DISA Computing Services Security Handbook, Section 3.1*.

3.2 Command Interpreter Monitor (CMON) Command-level Access Security Tool



Tandem - CMON Overview

Command Interpreter Monitor (CMON)
- TACL Auditing
- Restricts User-ID's Access
- Controls Shared User-IDs
- Heycmon
  – Start/Stop CMON Utility
  – Dynamic Configuration Maintenance
- Auditing Reports

GNOSC
DEFENSE INFORMATION SYSTEMS AGENCY
GLOBAL NETWORK OPERATIONS & SECURITY CENTER
ASYNC
CONNECTION(s)
TANDEM
CMON
AUDIT
LOG
$CMON
CMON
CTRL
FILE
TACL

Figure 3-1: Tandem CMON Overview

The Command Interpreter Monitor (CMON) is a process that is automatically called by a procedural exit in the Tandem Advanced Command Language (TACL) (the command-level user access interface to Kernel) when certain functions are executed by the user. In order to properly interface to the TACL procedural exit, $CMON must be the name for this process. This procedural exit allows for customized security enhancements and auditing for the command-level user interface. The $CMON process would usually be started as a part of the normal system initialization procedure (Command Interpreter Input [CIIN] file), or optionally as a part of the normal system startup obey files that are manually executed immediately after the normal system initialization completes.

If a $CMON process is not executing on the site, there is a vulnerability because any user or process with access to the site could start a new process and name it $CMON. Normally the TACL command-level user access processes running on the system trigger the procedural exits that send a message to the $CMON process and wait for the appropriate response. The procedural exit is triggered when the TACL user requests the following commands:

- **LOGON**
- **LOGOFF**
- **RUN**
- **ALTPRI**
- **REMOTEPASSWORD**
- **ADDUSER**
- **DELUSER**

The appropriate CMON response choices could be to allow the user request, disallow the user request, override the user request with pre-established guidelines, audit the user activity, spawn alert messages, capture user security information, or any combination of these actions.

Although BOSS disables the TACL exits to $CMON in the processes it controls, a knowledgeable user with TACL access could re-enable the exits. In addition, there are certain cases where non-BOSS controlled TACL access exists.

The $CMON process has been developed by SSO Mechanicsburg based on the requirements defined and authorized by Field Security Operations. The SSO released version is the standard that will be installed and executed at all times at the sites. It is anticipated that $BOSS and $CMON will coexist without conflict. When the SSO-released $CMON process is available, it will be installed, configured, and secured according to *Appendix N, GOTS Product Security*. If there is a need to perform any further configuration, guidance should come from the SSO with the software.

The SSO has developed the $CMON process to provide the following capabilities:

1. Log all successful and unsuccessful logon attempts and command-level utility access attempts.

2. Respond to the VPROC Tandem utility with the appropriate version release and timestamp information that can be used for $CMON process verification.

3. If Safeguard is running on the system, prevent logging on to the system from TACL processes for the NULL.NULL (0,0) userid.

4. Monitor the relevant activity that occurs on the TACL processes not monitored by $BOSS (i.e., the terminals located in the secured area and TACL processes started by application exits).

5. Generate and log relevant audit information of activities that it is monitoring (sufficient to support security auditing of the access and user activity).

6. Immediately after starting and just before stopping, $CMON will log these events to the Event Management Service (EMS) and to $CMON's audit logfiles.

7. $CMON will restrict *shared* userids by requiring the user to first log on to an authorized dedicated userid prior to logging onto the shared userid.

8. $CMON audit log reports should be used to verify the configuration via the binder time stamp by executing VPROC on that file.

9. $CMON will have an interactive configuration tool provided by the SSO group to aid in flexibility.

The IAO and System Administrator (SA) will ensure the proper configuration of $CMON by verifying the following items:

1. It must execute with the name of $CMON.

2. It must execute with the CAID and PAID of SUPER.SUPER.

3. It must have all related data files, obey files, configuration files, object program file, and audit data files owned by SUPER.SUPER and secured as "OOOO" (*Appendix N, GOTS Product Security*).

4. The audit data in these $CMON logfiles must be reviewed in accordance with DISA requirements.

The CMON program was developed, maintained, and documented by the SSO personnel as authorized by Field Security Operations. This CMON is the standard CMON to be distributed to all sites for installation in order to meet the additional security requirements for the command-level users.

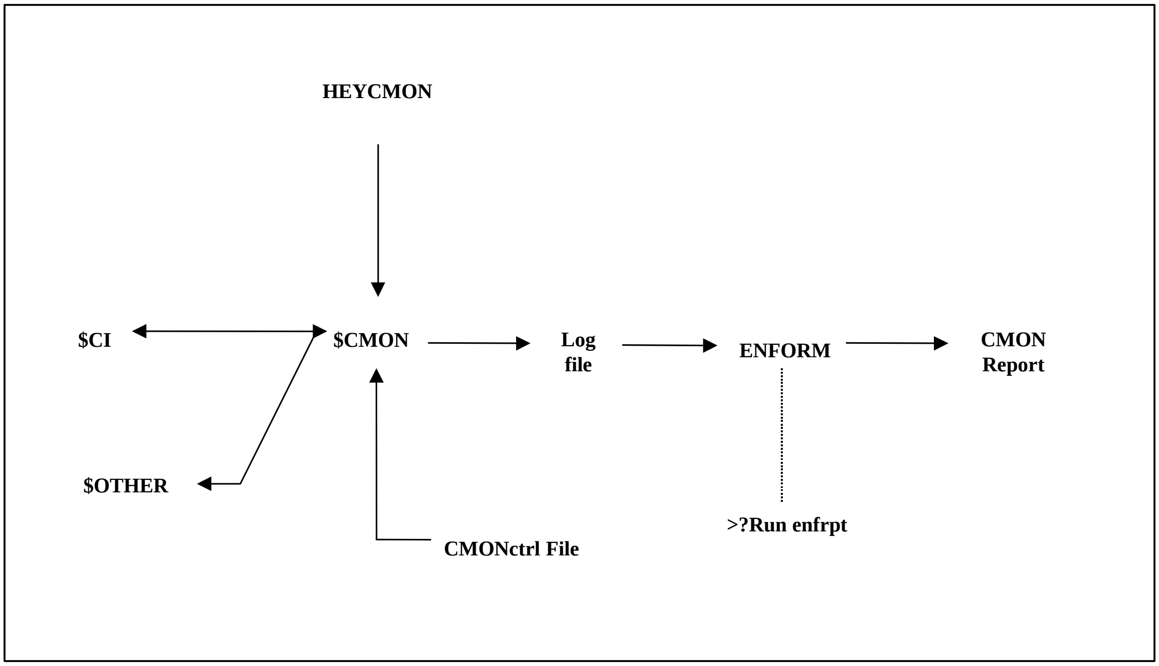
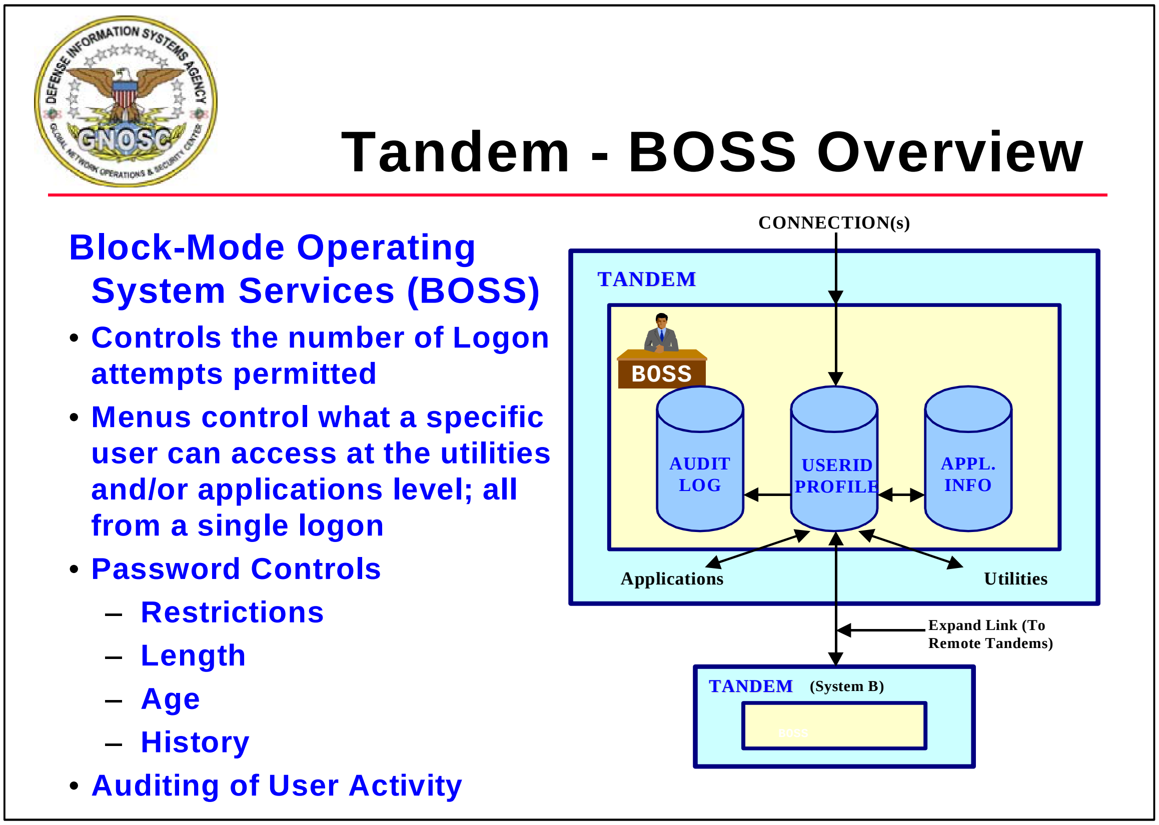


Figure 3-2: Tandem CMON Functional Diagram

- *The IAO will ensure that the current standard Field Security Operations-authorized CMON program is installed, properly configured, and executing with the name $CMON at the local site prior to allowing any user access to the Tandem system.*

3.3 Block Mode Operating Systems Services (BOSS) Security Tool



Tandem - BOSS Overview

Block-Mode Operating System Services (BOSS)

- Controls the number of Logon attempts permitted
- Menus control what a specific user can access at the utilities and/or applications level; all from a single logon
- Password Controls
  - Restrictions
  - Length
  - Age
  - History
- Auditing of User Activity

Figure 3-3: Tandem BOSS Overview

The BOSS-related information contained in this release of the STIG is based on the BOSS 4.0 version that was tested by SSO Mechanicsburg. BOSS, Version 4.0 or later, is anticipated to be the BOSS release that will be installed at the sites.

Initially, the BOSS product will be used to provide secure audited access control for application-level users and for most system-level users. BOSS must be configured to perform application user DAC and must audit all activity of the application user, as well as functions performed within the applications.

Care must be taken when defining userids in BOSS because BOSS does no validation on groupname/groupnumber or username/usernumber. Assign only one groupnumber to one corresponding groupname. Within a group, assign only one usernumber to one corresponding username. The userid for each user who will be authorized and executing remote node access need not be unique for each node in the network.

- *The IAO will ensure that the BOSS COTS product is installed and configured in accordance with DISA requirements prior to allowing any user access to the Tandem system. (See Appendix M, COTS Product Security, for specific settings.)*

- *BOSS will also be configured to audit the functions performed when accessing Kernel utilities, system administration, development, and operations functions from within BOSS.*

NOTE: See *Appendix O, Tandem Programs to be Audited*, for a minimum list of the utilities and functions to be audited.

- *Following the installation, initial configuration, and acceptance testing of the BOSS COTS product, the IAO will ensure that passwords associated with the default userids are changed prior to allowing any user access to the Tandem system.*

- *The IAO or SA will ensure that the default userid settings MACRO (DEFVOLSC) fielded by SSO Mechanicsburg (which resolves BOSS default userid settings) is in place and used.*

NOTE: See the e-mail message issued by SSO Mechanicsburg dated 09/22/2000 13:24 for specific detailed information. *Appendix P, BOSS Default Userid Settings*, also has information concerning this issue.

3.3.1 BOSS Application Profiles

Defining applications to BOSS includes defining the application profiles used to access each application, the domains used to group users with profiles, and the functions and flags associated with specific features to assign capabilities to each profile for users of the application.

The application profile can be set up to allow users access to specific application functions. SAs can use the application profile to limit the available application functions only to those the user requires. Application profiles can help the SA when setting up a group of users that require those application functions. For more information on application profiles, see the *BOSS Block-mode Operating System Services, User's Guide Version 4.0K, Section 4.2 Advanced Application Services*.

NOTE: Also see *Appendix E, "How To" Guide for BOSS*, for additional BOSS instructions.

For information concerning BOSS and Command-Level access Security Monitoring, see *Section 6.2, Command-level Access Security Monitoring*, in this document.

3.3.2 BOSS Domains

It is anticipated the IAO may want to delegate some of the user management functions to designated Domain Managers. This should be thought of as dividing users into groups called domains based on the applications to which users require access, the locations (potentially) of the users, and functions within the applications the users are authorized to perform. It may prove useful for the IAO and the Domain Manager(s) to preplan which users best fit into which domain based on what application access is required by the users, and what functions can be best grouped together for defining the application profiles.

To accomplish this within BOSS, the IAO must first define and name the domain(s). Next, the IAO must define the Domain Manager for each domain and the related MenuInfo File Maintenance records for each Domain Manager. Next, the IAO must define all Domain Application Info records and related profile information in each domain.

The Domain Manager(s) can then create the Domain Menu records and assign them to each user in that user's domain. After the Domain Manager has been defined to BOSS by the IAO, the remaining user maintenance functions (e.g., Domain BOSSid file maintenance, Domain/Profile file maintenance, password reset, and user directory services) for users in a specific domain can be performed by the manager for that domain.

NOTE: The IAO should consider the use of the Domain feature in BOSS to delegate application user management to an IAO-appointed Domain Manager.

- *If the domain feature is used, the IAO will ensure that the BOSS Manager creates all domains, and defines all entities for each domain to be used in BOSS.*

- *If the domain feature is used, the IAO will delegate the authority and responsibility of domain management to an IAO-appointed Domain Manager after the domain has been created.*

3.3.3 Remote Application Access through BOSS

To address the situation where a user needs access to some applications on a remote node, the remote access event must be recorded at the site where the application resides. The user will also be required to log on to the remote site prior to being provided a BOSS menu from that remote site. The remote site BOSS menu will only contain applications and functions that the remote site IAO has authorized the Domain Manager to configure for the users for which the Domain Manager is responsible.

The BOSS Domain Manager will control the remote site BOSS applications and functions menu options. The BOSS Domain Manager will pre-establish all remote domains that are allowed on the site. The BOSS Manager will create separate domains for each separate remote site where users exist that are authorized access to the site. The specific applications and functions that are authorized for all users at each specific remote site will be defined to the appropriate remote domain.

It may prove advantageous for the Domain Manager of a remote domain to be physically located at the remote site (where the user members are located).

- *If the domain feature is used, the IAO will ensure that a Domain Manager is assigned to each remote domain.*

- *If the domain feature is used, the Domain Manager will be located at the same remote site where the users are domain members.*

- *If the domain feature is used, the IAO will create BOSS domains and menu items to be used by the Domain Manager to configure and restrict remote users accessing the local site on an as required and authorized basis.*

3.3.4 Non-BOSS TACL Access

It is possible that a bug or other failure within BOSS, or some other system-level problem, could cause BOSS to hang, effectively disabling the system interface. Therefore, there is a need for non-BOSS TACL access from the devices located in a restricted area. The activity performed from these devices and access obtained must be controlled and audited using $CMON. If Safeguard is installed at the site and it does not impede production processing, it is strongly recommended that Safeguard also be used to aid in securing access through these controlled devices.

- *The IAO will ensure that there are two terminals located in a restricted area with TACL access not controlled by BOSS.*

- *One of the non-BOSS TACL terminals will be named in the System Configuration File* ***CONFTEXT*** *in the* ***ALLPROCESSORS*** *paragraph at the* ***SYSTEM_TERMINAL*** *parameter.*

- *The non-BOSS TACL terminals will be located in a secure area and have the following characteristics in accordance with DISA requirements:*

  - *They are physically located in a restricted area where only authorized personnel have access.*

  - *They are directly connected to the Tandem system via hardwired asynchronous (ASYNC) ports.*

- *They are maintained in a state with the TACL processes logged off.*

- *They are only used in critical or emergency situations.*

- *They are only used by authorized personnel.*

- *The TACL processes are executing in separate Central Processing Units (CPUs).*

- *The TACL processes are executing at priority 199.*

- *The two TACL processes will have swap volumes on separate volumes where the volumes are independent of each other in case of a CPU or controller failure.*

- *The TACL processes that will be executing on these two terminals in a restricted area (not controlled or monitored by $BOSS) will be controlled and monitored by using the CMON software.*

3.4 Safeguard Security Tool

Safeguard is a Tandem security and auditing product that runs in conjunction with Kernel to perform system-level security. Safeguard's monitoring features (SMON and CSNP) run as separate processes that can be started in one of three different ways depending on the level of security and the operational flexibility the site requires.

3.4.1 Safeguard Issues Related to Cold Load

The following list describes three approaches to using Safeguard:

1. The most secure installation approach is to configure (SYSGEN) Safeguard onto the system. This causes the entire cold load of the operating system image to abort if Safeguard cannot be started during the cold load.

2. A slightly less secure approach is to start Safeguard as a step in the normal system initialization procedure (CIIN file) that is automatically executed by Kernel immediately after the operating system image cold load completes. This method potentially could, but normally does not, allow for manual intervention. Manual intervention would need to be preplanned or an interruption during the system initialization is prevented.

3. Another approach is to start Safeguard in the normal system startup obey files. This is a system operator manually executed procedure (after the normal system initialization) to ensure that all (necessary applications and system) tools are appropriately executing prior to allowing user access. This method could easily allow for a manual interruption in the normal operations of the system and a potential lapse in security.

The approaches described in options 2 and 3 above provide an opportunity for dynamic shutdown of Safeguard while allowing the operating system to continue to process. They also provide the opportunity for Kernel to be executing without Safeguard running at startup time.

If Kernel is executing without Safeguard running, Safeguard-protected objects will not be secured, and a potential exposure to the database files that are normally monitored by Safeguard does exist. This security exposure is that Safeguard secured files could be controlled differently by Enscribe than the desired Safeguard configured security settings. Enscribe, allowing only the owner of a file, the owner's group manager, and the super ID to have access to a file does this. This exposure can be slightly more secure than the normal Enscribe file system security implemented when not using Safeguard. However, the advantage of using the options that allow Kernel to execute without Safeguard running provides the SA an opportunity to debug potential Safeguard problems and the ability to rule out Safeguard as part of a system-level problem.

If Safeguard is installed at the site, it does not impede production processing, and its use is planned to aid in security management. It is recommended that Safeguard be implemented using option 2 above because the advantages are considered to outweigh the disadvantages.

3.4.2 Safeguard in Conjunction with Enscribe Security

In the file header information for each file stored on disk, Enscribe has a Safeguard enable flag called the Safeguard security bit. When enabled, this security bit can provide additional file security as configured within Safeguard. To ensure this security bit is automatically set, an entry will be established for each user's default ACL in Safeguard containing this specification.

If Safeguard is installed at the site, if it does not impede production processing, and if its use is planned to aid in security management, to ensure proper security management, it is strongly recommended the Safeguard security bit be enabled on all critical files. Examples of files considered critical include the following:

Production Application Files

- Database files
- Obey files
- Command files

TACL Macros

System Executive Software Files

- Production tape management files
- Production NetBatch files
- Production Pathway files
- System startup files
- Operating system configuration files
- All Spooler files
- All system administration files

It is also strongly recommended that all Tandem command-level users have a Safeguard user's default ACL entry to force the Safeguard security bit to be automatically set for all files created by the users.

This page is intentionally left blank.

4. TANDEM SYSTEM SECURITY FUNCTIONS

4.1 Identification and Authentication

This section addresses the Identification and Authentication (I&A) criteria necessary to ensure that access to system resources is effectively managed and controlled for the Tandem systems.

4.1.1 Logon Warning Banner

Criminal court cases involving unauthorized access to official Government computer systems has prompted the need for a logon warning banner to be presented to anyone accessing a Government computer system. Logon warning banners or a legal notice of display must be displayed on all DOD devices in accordance with the *DISA Computing Services Security Handbook, Section 3.26.*

- *Logon Warning Banners will be deployed on all display devices allowing access to the Tandem (e.g., application or command-level access).*

- *The IAO will ensure that the* ***Legal Notice Logon Warning Banner*** *includes the four points outlined in the 16 January 1997 message from Assistant Secretary of Defense, Subject: Policy on DOD Electronic Notice and Consent Banner. All DOD AISs will display, as a minimum, an electronic "logon notice and consent banner" that advises users of the following principles:*

    - *The system is a DOD system.*

    - *The system is subject to monitoring.*

    - *Monitoring is authorized in accordance with applicable laws and regulations and conducted for purposes of systems management and protection, protection against improper or unauthorized use or access, and verification of applicable security features or procedures.*

    - *Use of the system constitutes consent to monitoring.*

- *The IAO will ensure that when the* ***Legal Notice Logon Warning Banner,*** *identified below, is not used, the banner being used has passed legal review from the appropriate DOD Inspector General (IG) office or Department of Justice (DOJ).*

The following is the DISA Field Security Operations recommended warning banner. A compressed version may be used as long as all of the criteria above are met.

LEGAL NOTICE LOGON WARNING BANNER

> THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED US GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING, TO ENSURE THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM, MAY BE MONITORED.
>
> USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

4.1.2 Logging On

Access to the Tandem system is controlled through the Kernel userid I&A logon function. Based on the security privileges granted to users when they log on, the user is granted a level of Object Access Control. Object Access Control is then propagated to any object the user accesses, regardless if it is a process the user starts, data the user wishes to create or access, or a function the user executes. If a user starts a process and that process starts a subordinate process, Kernel controls and propagates the user Object Access Control security authorization. This security authorization information is passed to the subordinate process in the form of the Process Access ID (PAID), the Creator Access ID (CAID), the related Enscribe file system security, the file owner ID assignments, and potentially the related Safeguard ACL assignments. This further ensures that a user cannot appear to be another user for authentication and granting of an unauthorized level of access or privileges.

The need may arise for System Administration group users, System Operations group users, Help Desk group users, SSO group users, and CDA group users to log on to userids that must be shared. The shared userids are only to be used for administrative purposes by authorized users. When accessing the system through the Non-BOSS TACL terminals (CMON), the users with authorization to the shared userids must first log on to their own unique userid prior to logging on to the shared userid. When accessing the system through the BOSS application, a menu item should be added to the authorized users allowing them to execute an Audited TACL that is run as the userid of the shared userid.

- *Users will log on to the system with a unique userid (groupname.username) and password.*

- *Users will not be able to log on to another userid without the password for that other userid.*

NOTE: Users that are connected to a BOSS terminal will not be allowed to logon as another userid. A RUN-AS menu-item will need to be configured for the user.

- *When BOSS fails, for any reason, and is unavailable to perform I&A, the IAO/SA will ensure that all application access is also unavailable and remains unavailable until BOSS is available to perform I&A.*

- *Users will log on with their userids and will not be able to log on using their userid numbers.*

- *The IAO will approve all administrative shared userids, and will ensure that shared userids are only accessible from previously logged on TACL and/or BOSS interfaces.*

NOTE: The only shared userids on the system will be administrative shared userids for specified groupnames and each will be documented and approved by the IAO.

- *The IAO or Domain Manager will ensure that only authorized users will be set up to run as a shared userid.*

NOTE: BOSS users will not be allowed to log on a shared userid. Users that need access to a shared userid will be required to have a menu item configured to have the TACL entry set so the RUN AS parameter is set to the required shared userid.

- *Only authorized users will have access to the password(s) of the specific shared userids to which they require access.*

4.1.3 Logging Off

An interactive command-level access session to the Tandem system is terminated when the user **LOGOFF** command is executed.

- *The IAO will establish local policy to ensure that users* ***do not*** *leave their unsecured Tandem sessions unattended, and they log off the Tandem computer whenever they need to leave their unsecured terminals.*

4.1.4 Guidelines for Strong Passwords and Userid Locking

Restrictions must exist to ensure each user has a unique logon userid and password. Each userid has a predefined expiration date and will be suspended from use if expiration date is passed. They will also be suspended if the threshold for excessive invalid sequential logon attempts has been exceeded. Minimum password length, password reuse restrictions, password encryption, suspension guidance, and an excessive number of invalid password attempts lockout threshold, normally three, will be enforced in accordance with the *DISA Computing Services Security Handbook, Section 3.13*.

- *BOSS will be configured to suspend the userid after the threshold for consecutive failed logon attempts has been exceeded.*

NOTE: The freezing of a userid in BOSS requires manual intervention by an authorized Security Administrator to thaw the userid.

The BOSS product and the Safeguard software have the ability to interact while addressing system security issues, thereby complementing each other. If both products are in use simultaneously, they should be configured in a non-conflicting supplemental manner to aid in the support of the overall security concept for the Tandem system. BOSS is capable of securing the application logical userids along with some of the security aspects for the Kernel userids. Safeguard is capable of providing security restrictions for Kernel userids as well as other system resources (administered and managed as objects).

- *All Kernel and logical application userids will be established and maintained using* ***strong password*** *restrictions.*

- *Passwords will be encrypted when stored on the system.*

- *Passwords will have a minimum length of eight (8) alphanumeric characters with at least one (1) numeric character and one (1) alphabetic character.*

- *Passwords will not be echoed to the screen.*

NOTE: The only time it will be valid for command-level logon passwords to be entered from the user is when the user is prompted for it.

- Users are permitted to manage their own passwords and will change their passwords every 90 days.

- *Passwords will not be changed more frequently than once every 24 hours without intervention of the IAO.*

- *Passwords will not be reused within ten (10) password changes.*

When three consecutive invalid logon attempts, occur to non-BOSS terminals, Kernel forces a delay of 60 seconds (non-configurable) after every subsequent invalid logon attempt. This delay continues to occur until the next valid logon. The actual requirements for lockout of userids are as follows:

- *All successful and unsuccessful logon attempts will be logged to an audit file.*

NOTE: Be aware that this may cause a large amount of audit data to be generated because the operating system and related components execute under the SUPER.SUPER userid. These parameters must only be enabled for the SUPER.SUPER userid for a limited time unless large amounts of spare disk space are available to contain the audit trails.

- *The TACL userid will be locked out of the system after three consecutive unsuccessful login attempts.*

4.2 Discretionary Access Control

This section discusses the Discretionary Access Control (DAC) and *least privilege* resource access and implements a need-to-know policy by restricting the user's access to file or system objects as determined by the custodian of the data (usually the IAO). All users must be established with a unique userid and password in accordance with the *DISA Computing Services Security Handbook, Section 3.13*.

- *All Kernel userids will be created with an initial password the user must change immediately upon logging on to the system for the first time.*

- *The IAO will establish local policy to ensure that users do not share userids and passwords.*

- *All application users will have a unique application userid.*

- *All command-level users of the local Tandem system will have assigned to them at least one unique Kernel userid, where all command-level functions they perform will be executed under that userid.*

When it comes to the users in BOSS, you can have access to BOSS and TACL without being an NSK user. If possible, you should only define a user to be an NSK user if required. There are some cases where the operator (e.g., Operator.John) is on a shift and another operator does the same job on a different shift. You can set them up with unique BOSS userids and have them do a Run As. This will work if the TACL is audited.

- *The IAO, or their appointed representative (Domain Manager or Functional OPRs), will determine the appropriate level of access for each user (full TACL command-level access, limited TACL command-level access, or application access).*

NOTE: Level of access will determine what data you will be able to view and/or modify. One user may be able to update the database and another may only be able to view the information.

- *The IAO will ensure that the appropriate assignment of an internal application User-to-Function matrix or BOSS menus and submenus user access levels is defined as required.*

- *The IAO will determine which capabilities will be allowed for the limited command-level access BOSS menus or submenus and which userids will be allowed to access these menus or submenus.*

It is possible for an application to provide user accessible exits from the application to TACL and command-level utilities. When the application user has exited from the application to the command-level utility or TACL, the user has the functionality of a command-level access user. Therefore, to allow for system-level I&A, all command-level utility and TACL processes executed on behalf of that user (after exiting from the application) are required to execute under the unique Kernel userid that was pre-assigned to that user.

In the case where the CDA software supports multiple sites, Field Security Operations will also maintain the relevant security agreements. This is to assure the applications do not have system utility or TACL exits except as documented, and the processes accessed by the application users are executed under the predefined Kernel userid that will be unique for each user that accesses these exits.

4.2.1 Defining Userids, User Groups, and Special Groups

User-level integrity is addressed within the Kernel implementation of a group and userid assignment strategy. The Tandem SA assigns users to a group and userid. The separation of users consists of securing the system-level access and the application-level access, implementing password protection, monitoring user access, and maintaining satisfactory performance. The following sections discuss each of these in detail.

Kernel associates every userid with one specific userid group. There are 256 available userid groups on each Tandem system. There are 256 available userids for each userid group on each Tandem system, for a total 65,536 possible userids.

4.2.1.1 SUPER and NULL Groups and Users

Tandem has two special userid groups that require extra consideration. These are the super-group (255,*****) and the null-group (0,*). The super-group must be strictly administered and audited to ensure appropriate levels of security are maintained. Of the super-group, one userid will need to be reserved for the Tandem System Engineer's use. This super-group userid used by the Tandem System Engineer must be maintained with strong passwords. There are two userids in the null-group, at the sites, that will not be allowed to log on to the Tandem systems. Those userids are 0,0 and 0,255. The only exception is for the SAs to change the password every 90 days. If Safeguard is not running on the system, the null-group null-user and administrator (0,255) userids will be removed from the system.

- *When Safeguard is not running on the system, the NULL GROUP User (0,0) and the NULL GROUP Administrator (0,255) userids will be deleted from the system.*

- *When Safeguard is running on the system, the NULL.NULL userid (0,0) will be deleted and replaced with the NULL.BOSS userid (0,0).*

- *When Safeguard is running on the system, the NSK 0,0, and 0,255 (if required) userids will be secured with strong passwords.*

- *When Safeguard is running on the system, the NSK null-userids (0,0 and 0,255 (if required)) will be secured at all times and will not be defined in BOSS.*

- *When Safeguard is running on the system, all activity done under the NSK 0,0 and 0,255 userids will be audited, and reviewed by the IAO.*

- *When Safeguard is running on the system, the IAO will establish local policy to prohibit logging on as either NSK 0,0 or NSK 0,255.*

- *The IAO will ensure that the super-group userid used by the Tandem System Engineer (without appropriate security clearance) is secured (suspended in BOSS) at all times, except when the Tandem System Engineer is working on the local site.*

- *The password for the super-group userid used by a Tandem System Engineer (without appropriate security clearance) will be changed immediately after the Tandem System Engineer is done on the system and secured at the site so no one can log on to this userid.*

NOTE: The new password for this userid will be provided to the Tandem System Engineer the next time access is required.

- *The super-group userid, used by the Tandem System Engineer, will be secured and maintained with strong passwords like all other userids.*

4.2.1.2 Administrative User Group

There will be a Tandem Kernel user group (e.g., **255,***) for System Administration. This user group is referred to in this document as the Administrative group. The users included in this group may come from several different organizations within DISA or the site. The Administrative group users are those who have the function of the SA, Database Manager, Data Communications or Network Manager, and the IAO. The Administrative group users are given special security-related access, administrative responsibilities, and privileges. Auditing and review of administrative user activity must be performed in accordance with the *DISA Computing Services Security Handbook*, *Section 3.3*.

- *Functions executed by the Administrative group users will be more closely monitored and audited than* ***standard*** *users.*

4.2.1.3 Group Manager Userid

Tandem also has a special userid (*,255) in each user group that requires special consideration. This userid is known as the Group Manager. The Group Manager userid for all userid groups will be used only in one of the two following cases, with the exception of the manager of the Super group:

- The on-line and batch application server and requester processes that allow application-level access for users to the application database, and run under the management of the Pathway monitor

- For userid group administration

- *The IAO will ensure that the Group Manager (****,255***) userid for all userid groups is used only for the application processes and the management of the related pathway or for the groups administration.*

4.2.1.4 Group Separation

Each user that requires command-level access must be assigned a unique Tandem Kernel userid. As an extra level of security, each user department of the applications that reside on the Tandem system could have a unique user group assigned to it. Exceptions would be when more than one user department needs to access only a single application, the total number of users accessing the single application exceeds 254, or the number of unique user groups available on the system does not allow for this level of user group separation. For exceptions to implementing this user group separation, contact Field Security Operations for guidelines.

Due to the special functions and extra capabilities of the super-group, the Administrative group, the Group Manager, and the null-group userids, closer than normal monitoring and auditing must be performed for any access or function performed by these userid and group members.

If the three groups of userids (super, administrative, and null) and the one Group Manager userid are excluded, Tandem Kernel can support up to 64,262 userids per system (groups #1-253 = 253 groups times 254 users per group = 64,262 users per node). Therefore, if each application has a separate userid group, each node can support up to 253 groups (applications) of 254 users per group.

The idea is to have a logical grouping for users in an attempt to simplify the user management function. For example, a specific Kernel userid group could be assigned to a DOD program group or department. In addition, a specific application subsystem access could be assigned to a specific set of Kernel userid groups. Thus, the IAO can restrict application subsystem access to a specific set of Kernel userid groups. In addition, the IAO can restrict a Kernel userid group to a specific set of application subsystems. This can be accomplished by having each DOD program group or department assigned to only one userid group if possible (less than 254 users per program group).

It is possible that a single userid group may be used by more than one program group or department if the program group or department has a common need to access the same application subsystems, and the total users that need access for this group can be 254 or less.

- *When assigning a new Kernel command-level userid and group ID to a user, every attempt will be made to carefully choose the group ID being assigned so it aids in the logical grouping of users.*

NOTE: This will minimize the effort required when performing user management.

4.2.2 System-level Access Control

System-level security access control consists of protecting both local and remote access of command-level users for both full TACL and limited command access. The following four parameters will be set to ensure password restrictions are enforced for all levels of system command-level access using TACL and COMINT:

- ENCRYPTPASSWORD	ON
- BLINDPASSWORD	ON
- MINPASSWORDLEN	8
- PROMPTPASSWORD	ON

NOTE: The PROMPTPASSWORD will be set to OFF in the Password program collocated/used by BOSS.

The following TACL parameters will be set for the non-BOSS terminals to ensure access restrictions are enforced:

- AUTOLOGOFFDELAY	ON (15 minutes)
- CMONREQUIRED	OFF
- CMONTIMEOUT	(30 seconds)
- BLINDLOGON	ON
- NAMELOGON	ON
- NOCHANGEUSER	OFF
- REMOTECMONREQUIRED	OFF
- REMOTECMONTIMEOUT	(30 seconds)
- REMOTESUPERID	OFF

- *The password and TACL parameters will be set for all TACL processes.*

The IAO should establish procedures to ensure the only full TACL users with EXPAND network access are those with direct connect terminals in secured areas, or through access from the Trusted Network.

4.2.2.1 Local Kernel Userids

Kernel associates a unique groupnumber (0 through 255) and usernumber (0 through 255) with each Kernel user groupname and username as defined by the SA or IAO.

4.2.2.2 Full Kernel Command Level Access

TACL, the standard command-level access interface to Kernel, hereinafter referred to as full TACL, is used to access the system administration utilities. COMINT is the old standard command-level interface to Kernel and, if still in use at the sites that use EXEC, must be phased out as soon as possible. For a command-level user to gain access (logon) through TACL or COMINT, it is required that the user provides a valid predefined Kernel userid and password. In this document, when reference is given to Kernel command-level access interface, this includes both the COMINT and TACL tools.

Kernel provides four standard levels of user access, which are comprised of SUPER.SUPER, super-group member, (non-SUPER) Group Manager, (non-SUPER) group member, or basic level user. All four standard levels of user access provided by Kernel are capable of full Kernel command-level access from TACL or COMINT. However, please note the four standard user access levels have different predefined functions they can perform. The highest level of access is granted to the SUPER.SUPER userid. The remaining super-group members have specific functions that only the super-group is allowed to perform. The non-super Group Managers have other specific functions that only the managers of each specific group are allowed to perform.

Once the user has successfully completed the logon procedure for TACL, that user is provided with command-level access to all resources on the Tandem systems the user is entitled to access based on their security level. Full TACL includes potential access to system management tools with capabilities such as the following:

- Configuration management
- Enscribe file management
- Database management
- Print Spooler and spooled report configuration management
- Hardware configuration management
- Communications configuration management and traces
- Application subsystem configuration management
- Software development (including compilers and debuggers)
- Data monitoring
- Software traces
- Auditing
- Security configuration management

- *The IAO will ensure that full TACL access is only available through direct connect terminals in secured areas, through access from the* ***Trusted Network****, or through an encrypted connection between the terminal and the Tandem.*

4.2.2.3 Dial-up Security

If dial-up access is active on the Tandem, then dial-up security will be accomplished by using a second copy of BOSS (Stand-alone) that is used to manage the dial-up ports only. This second copy of BOSS needs to be configured exactly like the primary copy of BOSS with the following exceptions:

1. The only terminals supported are those authorized to use the dial-up ports.

2. The only users supported are a small subset of the Administrative group authorized for dial-up access.

3. The only unit of work supported is a minimum predefined set of functions.

Everything in this second copy of BOSS must be closely audited and monitored in accordance with DISA requirements and local INFOCON Level Guidance. The goal is to minimize exposure to a potential attack through dial-up access by limiting the number of users that can dial up, the functions these users can perform when accessing through dial-up, and only allowing dial-up access when absolutely necessary. The existence of a dial-up access, without satisfactory extra measures, will be considered a potential security risk if it is not properly secured. Additional information can be found in this STIG in *Section 10.7, Dial-up Access and External Phone Line Connections*. More detailed information on this subject can be found in the *Network Infrastructure STIG*, the *STIG on Enclave Security*, and the *DISA Computing Services Security Handbook.*

- *The IAO will work with the Network Security Officer (NSO) to ensure that the Trusted Network (an internal site network) is STIG compliant and does not include paths across the* *common user backbone.*

- *The IAO will establish procedures to ensure the System Administration group access is only available through direct connect terminals in secured areas, through access from the Trusted Network, or through an encrypted connection to the Tandem.*

- *When dial-up exists on the Tandem system, dial-up security will be established by using a second copy of BOSS (Stand-alone) to manage all the dial-up ports only and limit access to a subset of authorized users and minimal subset of necessary functions (units-of-work).*

- *When BOSS is not being used to control and audit the dial-up ports on the Tandem, the dial-up processes will be terminated and not used until BOSS can be configured to control and audit the dial-up ports.*

4.2.2.4 Kernel Limited Command-level Access

Kernel limited command-level TACL access (hereinafter referred to as limited TACL) allows users to access some system utilities or functions and restricts access to others. BOSS is going to be used to provide users with a limited TACL access and to control what utilities, commands, or sub-commands the limited TACL users can access through their menus or submenus.

- *The IAO will establish guidelines for limited TACL and its limited access users to include the following restrictions:*

  - *They are not allowed to set or modify their own default security settings or default volume and subvolume.*

  - *They will have full access to their own TACLCSTM files.*

  - *They will not have access to the following COTS/GOTS products:*

    LITECOM
    ENLIGHTEN
    FOCUS
    BOSS

- *All production processes will have a pre-defined home terminal (e.g., Virtual Home Term) so Inspect and Debug prompts do not go to the user's terminal.*

- *The Kernel limited TACL will not allow users to execute a set list of tools unless approved and documented by the IAO.*

ADDUSER
AID
AXCEL
BACKUP
BIND
C
CMI
CMON
CMP
COBOL
COBOL85
COMINT
COUP
CROSSREF
CUP
DDL
DEBUG
DELUSER
DCOM
DISKGEN
DIVER
DNS
DSAP
DSC
EDIT
EMSCOLLECT
EMSDIST
ENFORM
EXEC

FASTSORT
FTP
FUP
GPA
IMON
INET
INSPECT
INSTALL
LISTENER
LOAD
LOGON (New)
MEASCOM
MEASMON
MD2
MIO
NETCOM
PAL
PASCAL
PASSWORD (New)
PATHCOM
PATHMAKR
PATHMON
PATHTCP
PEEK
PMINSTALL
PUP
RECEIVEDUMP
RELOADCPU
REMOTEPASSWORD

RESTORE
RJECI
SCF
SCOBOL
SCOBOLX
SORT
SCUP
SPOOLCOM
SQLCI
SQLCOMP
SYSGEN
TACL (FULL)
TAL
TANDUMP
TAPECOM
TCPIP
TEDIT
TELNET
TELSERV
TGAL
TMDS
TMFCOM
UPDATE
VIEWPT
VIEWSYS
XRAYCOM
XRAYSCAN
XREF
XVS

- *The IAO will create and maintain a list of functions that the local limited TACL users will be allowed to access.*

- *When the suggested list of functions is expanded for the local users, the additional access is documented and approved by the* IAO.

  - *The suggested list of functions available to the limited TACL users is as follows:*

    BACKUPCPU
    LOGOFF

    PERUSE
    STATUS

    SWITCH
    TIME

4.2.2.5 Remote Kernel Command-level Access Userids

The following three main controls are related to remote access:

- Remote Kernel userids (group, user, names, and numbers)
- Remote passwords
- Remote Enscribe security

NOTE: Remote Enscribe file security is addressed in *Section 4.2.4, Default Users File Security Settings*.

- *The local IAO or the SA will set all userids and **REMOTEPASSWORDs** for all remote access to the local site, if access has been approved by the local IAO.*

4.2.2.5.1 Remote Kernel Userids

Remote Kernel users are required to follow the same Kernel and Safeguard access rules that apply to local command-level users. Additionally, before remote access is possible for a user, the Administrative Group Manager must obtain authorization from the IAO, and pre-establish REMOTEPASSWORDs with associated matching userids at each node to which the user requires access. Remote file security must also be appropriately set for all files to be remotely accessed.

4.2.2.5.2 Remote Passwords

The REMOTEPASSWORD command is a TACL command to allow a specific user to establish a session between two Tandem nodes. This command must be executed for each user that requires access, and on each node, the user needs to access.

4.2.3 Application-level Access (Integrity) Control

Application integrity and availability are addressed in the following sections as they pertain to the Tandem implementation. Tandem provides a fault tolerant hardware and software design in a modular fashion, allowing for separation of functions and multiple concurrent processing. To take advantage of this feature, the CDA must design and develop the Tandem applications programs to run under Tandem's standard Pathway product, use Tandem's standard TM/MP for data transaction auditing, or be coded with NonStop programming.

The careful management and monitoring of SETMODE, CONTROL, CONTROLBUF, escape sequences, and sequential input/output (I/O) procedure function programming commands are required to ensure security. These programming functions could potentially cause a compromise in the C2 security base. Therefore, they must not be used in normal applications software, unless specific requirements exist and approval is obtained from Field Security Operations prior to production installation. When these powerful functions are executed by an application, agreements must be maintained documenting that the related security issues are being maintained in accordance with the *Computing Services Security Handbook.*

- *The IAO will maintain local agreements with the CDA to provide assurance that there are no undocumented SETMODE, CONTROL, CONTROLBUF, escape sequences, and sequential I/O procedure functions programmed in the application.*

- *The IAO will maintain local agreements to document the security responsibilities accepted by the CDA for application users access when specific functions are programmed into the application:*

NOTE: The list includes SETMODE, CONTROL, CONTROLBUF, escape sequences, and sequential I/O procedure functions. The agreements will ensure that whenever an application performs one of these functions, it does so while maintaining the necessary security guidelines.

4.2.3.1 Application User Mapping to a BOSS Logical Userid

Application-level user access must be mapped to a BOSS logical userid. BOSS requires the logical user to enter a group ID, userid, and password before the user can gain access. The application-level access provided to the logical user has specific rights (*read, write, execute, purge/create,* and *owner*) to one or more application and database tables as determined by the IAO in accordance with the DAC requirements.

The application-level logical user must not have direct access across the EXPAND network. The only allowed network access for this level of user is from within an application process (requester/server) executing under the application owner userid or pre-assigned Kernel userid. The remote access for this application owner userid must be authorized by the IAO on a DAC level before it is established. REMOTEPASSWORDs are established only for the application owner userids that must access remote nodes.

- *The IAO will ensure the application users are restricted so they do not have direct remote access.*

- *The IAO will establish and manage remote access for application owner userids only as needed, and will periodically review the need for these remote accesses to determine if any of them can be eliminated.*

- *The IAO will explicitly define the DAC levels for all remote access of application-level users.*

4.2.3.2 Application User Subsystem and Functional-level Security Matrix

Each application-level user's access will be limited to accessing the databases for that application through the standard applications interface. The application-level user's access is normally mapped to specific functions or rights (i.e., *inquire, update, add, and delete*) and to one or more applications (or a specific set of application subsystem processes and database elements) internally in the applications. It is anticipated that this functional-level access mapping can be configured for each user in BOSS from the applications to allow, for security administration, to occur at a higher (global) level. BOSS is expected to manage, control, and audit the actions (i.e., *inquire, update, add,* or *delete*) that a user can perform from within an application by using the advanced auditing, functions, profiles, and flags features of BOSS. Legacy applications that perform functional-level security access with the application are acceptable. Any new application will use the BOSS features described above.

- *The IAO will ensure that advanced auditing is enabled for tracking function-level access mapping activities and will periodically review and maintain these user application capabilities to ensure up-to-date application security and data integrity.*

Further granularity of (data element-level) access privileges are addressed through NSSQL, and are further discussed in *Section 5.6.1, Database Management System Security*. The Security Administrator group establishes this granularity in conjunction with a Database Administrator, through evaluation and DAC review.

To test application-level user mapping, the SA or IAO can log on to several different application user-level userids at the application logon screen and navigate through the application menus, looking at production data when available, to verify the users only have access to the appropriate data and applications. If anomalies are found, the application user-level access matrix can be updated and re-tested to determine if the problem is in the applications security matrix file or in the applications software.

To maintain data integrity and availability at a system level, the SA needs to be involved in the maintenance of the database to ensure TM/MP roll forward, backout transaction recovery, and system backup and recovery do not negate any file security settings as established by the IAO. This can be verified by creating a baseline backup and report listing of the database and file security following the initial database setup. This baseline must be replaced occasionally following major releases of software and/or database maintenance. If a question regarding database security or integrity arises following any event that could pose a potential security breach, or after a major system failure, the IAO can compare the most recent baseline report listing to the current database to verify the database structure, the file security, ownership, and access settings are appropriate.

- *Application-level user's access will be limited to the production databases by accessing through the designed production applications interface.*

- *The IAO will ensure that the current baseline reports and backups are maintained for recovery verification comparisons.*

- *The IAO will secure that the production databases with first the Kernel file system and then with any additional security packages.*

- *The file system security for stand-alone application databases will be set to "**OOOO**" so only the data owner has access to the data.*

- *The file system security for network-wide shared application databases will be set to "**CCOO**" so that only network-wide group members and the data owner have access to the data.*

4.2.3.3 Application Process Control

Application processes normally cannot be allowed to run as privileged processes because this defeats the system-level security. Therefore, special care will be taken when allowing programs to have their PROGID bit set or to be licensed.

- *Privileged programs will not be accessed internally from any application where the standard application user can access them, except where the IAO has documented the programs and user access.*

NOTE: The documenting of the programs and user access should include the following items and can be documented as part of the user application matrix:

- Name and location of the privileged program
- Owner and security settings of the privileged program
- Sensitivity of the program capability.
- Operational reason for the need to use the privileged program.

- *The IAO/SA will set the privileged programs on the system so they are audited in the audit logfiles.*

- *The IAO/SA will monitor the BOSS audit logfiles so that if any privileged programs have been executed without IAO/SA approval, then the appropriate incident reporting needs to be executed.*

- *Licensed programs and PROGID (owner id) programs will not be allowed to be set for any application where the standard application user can access them except where the IAO has documented the programs and user access.*

4.2.3.4 Application User Password Protection

All operating systems, certified as Class C2 compliant, must protect passwords from unauthorized users. Kernel allows specification of a password for each command-level userid. BOSS and Safeguard can also be used to aid in enforcing additional password protections. Also, for very sensitive applications and data, another layer of user I&A can be performed internally by the application to further audit users functions and force multi-layer logon access where required.

Certain guidelines must be followed for password creation and maintenance to ensure security measures are followed in accordance with *DISAI 630-230-19, DODD 8500.1 or CJCSM*. Minimum requirements for password length, repeat passwords, frequency of change, etc. must be followed. The sites must therefore enact and publish policy, consistent with *DISAI 630-230-19, DODD 8500.1, CJCSM,* and the *Computing Services Security Handbook.*

- *When BOSS is not being used to control the system-wide access, the IAO will maintain local agreements to ensure the password policy is followed.*

4.2.4 Default Users File Security Settings

The Tandem file management system security ensures the file owner and access security rules are implemented as initially established by the Administration group and maintained by the file owners.

These access security rules are file specific and are based on the four security parameter settings for each file (*read, write, execute,* and *purge*). These four file specific parameters can be set for local (A, O, G, **–**) or remote (N, U, C) access and can be set or modified on all files as required by the need to access the data.

Enscribe has four local file security values for the file security parameters that allow local access. These are A, G, O, and **–** and are defined as follows:

LOCAL SECURITY	***DESCRIPTION***
A (**Any)**	Access to any user in the local node where this file resides.
G (**Group) -**	Access to any user in the local node where this file resides and must be a member of the same user groupname and groupnumber as the file owner.
O (**Owner) -**	Access to only the file owner user in the local node where this file resides.
– (SUPER.SUPER Only)	Access to only the SUPER.SUPER user in the local node where this file resides.

Figure 4-1. Local File Security Table

- *The IAO will ensure that the default security for all NSK command-level users is set to "**OOOO**" (preferred) to allow only owner-level access to **read**, **write**, **execute**, and **purge**, or without an extension, the default security can be set to be no more permissive than "**GOOO**".*

Enscribe has three remote file security values for the file security parameters that allow network access. These are N, C, and U and are defined as follows:

NETWORK SECURITY	***DESCRIPTION***
N (Network)	Access to any user in the EXPAND network that has remote access established to the node where this file resides.
C (Community)	Access to any user in the EXPAND network that has remote access established to the node where this file resides and is a member of the same user groupname and groupnumber as the file owner.
U (User)	Access to any user in the EXPAND network that has remote access established to the node where this file resides, and has the exact same user and groupname and groupnumber as the file owner.

Figure 4-2. Network File Security Table

- *Local files will not be given network access security unless specifically requested, granted and fully documented by the IAO.*

NOTE: Depending on the application in use on the system, some files may need to have network access. Files that need network access should have the maximum security set so only those authenticated users have access. All other files should be secured away from network access.

4.2.5 Default Users Subvolumes

When the SA assigns a Kernel group and userid, it must have a default volume, subvolume, and security assigned to it. The volume and subvolume is the default location for storage of any files that are created by that user. The ability to change these defaults from the command-level interface must be restricted to the users of the System Administrator group.

- *The IAO will ensure that each command-level Kernel userid will have the default security, volume, and subvolume set before the user is allowed access to the Tandem system.*

- *The IAO will ensure that the default subvolumes will not be located on the $SYSTEM volume, the TM/MP audit trail volume, or the production data volumes except for the IAO approved and documented Super-Group users that require subvolumes on $SYSTEM.*

NOTE: If no other disk volumes are available on the system, the production data volume with the lowest anticipated workload should be used for the userid default volume. Each command-level Kernel userid should have a unique default subvolume unless there is an operational need and this need is approved and documented by the IAO.

4.2.6 Object Access Controls

Object-level integrity is addressed with Kernel and an additional granularity of security control can be provided using Safeguard. Kernel ensures that processes started by a user have only the access privileges of the user that originated them. In addition, a subordinate process (a process that is spawned by another process) has the same access privileges as that of the spawning process as though the original user started it. When properly configured, Safeguard can provide object-level access control using ACLs. These ACLs can control the Kernel userids, and can control the access to processes, devices, subdevices, disk volumes, disk subvolumes, and files. The Safeguard ACLs provide the ability to assign users into arbitrary groups, thereby supporting group-level access control. With Safeguard ACLs, an IAO also has the ability to explicitly deny or permit access by a userid or groups of userids. Safeguard writes audit data to a logfile of security access event information pertaining to activity it is monitoring.

- *The IAO will ensure that all sensitive data files are secured to include but are not limited to the following files:*

  BOSSID2
  USERID

NOTE: See also *Section 5.6, Database Reliability.*

- *The IAO will ensure that all individual userids, System Operators, System Administrators, and Security Administrators are subject to the DAC security mechanisms as assigned and implemented by the IAO.*

4.2.7 Resource Controls

4.2.7.1 Database and File Management Access Tools

Listed in this section are the standard database and file management access tools for Tandem systems. These tools include the following:

- FUP is used to manage files.
- DDL is used to define Enscribe file structure.
- SQLCI is used to define and manage the SQL database.
- DCOM and DSAP are disk maintenance tools.
- 4GL (4th Generation Language) tools are used to access the SQL databases with minimal programming efforts.

These tools are used to perform the necessary functions related to database and disk volume maintenance normally executed by a member of the SA group. Normal maintenance examples include clean-up of old files, initial database setup, database loads and reloads after special modifications or tests, updating database population statistics used to optimize queries, database and file tuning, and verification of the database status following recovery from failures.

- *Access to the database and file management tools will be limited to only those IAO documented individuals that require access.*

4.2.7.2 System Management and Configuration Tools

The standard Tandem system management and configuration tools are as follows:

- Peripheral Utility Program (PUP), which is used to manage hardware devices
- Transaction Monitoring Facility Command Monitor (TMFCOM), which is used to manage TM/MP
- SQLCI, which is used to manage the NSSQL databases, application catalogs, and system catalogs
- PATHCOM, which is used to manage application links
- SAFECOM, which is used to manage the Safeguard security tool
- BATCHCOM, the NetBatch interface tool
- DDL, which is used to create and modify Tandem libraries.
- TMDS, which is used to view/manipulate the EMS logfiles.
- SCF, which is used to manage communications on the system.
- CMI, which is used to manage communications on the system. Functions of this product are being replaced by SCF.
- CUP, which is used to manipulate devices on the system. This is normally when hardware is added or removed from the system without taking an outage. To remove hardware using this utility, the hardware must have been added using this utility.

These tools are normally used to configure and maintain the system, control access to resources, and reestablish the production environment during failure recovery.

- *The IAO will ensure that access is limited for the standard system management tools to only the SA group unless there is an operational need and this need is approved and documented by the IAO.*

NOTE: If there is a need, the IAO will ensure that access will also be available and documented for the tools (PATHCOM, BATCHCOM, and NetBatch) to those members of the SSO group and the CDA group that have a requirement to access these tools.

4.2.7.3 Tape Processing

The standard labeled tape processing must be enabled, a tape management software package must be installed, and the tape management function must be performed to manage and create an audit record of backup tapes and other tapes containing production data or critical software. This can assist the IAO and the SA group in the management and auditing of tape processing in accordance with the *DISA Computing Services Security Handbook, Section 3.12.*

- *The IAO and the SA will ensure that local policy addresses the need for the tape management function to be performed.*

4.2.7.4 Software Development Tools

For several reasons, it is important not to have production and development occurring on the same system. Separate development systems provide more flexibility for testing applications, tools, COTS, and operating system software. Separate systems can reduce the probability of an attack on the system. Separate systems assist in providing better software version control. When a system is only used for production, it is important to prevent inadvertent or malicious use of the development tools from occurring on that system. This can be accomplished by controlling access to the development tools.

When production and development must occur on the same system (referred to as a mixed system), it becomes a more difficult task to guarantee the stability of the software installed, and to prevent the introduction of untested or potentially malicious code. Therefore, to control the software environment, extra precautions will be taken to ensure only authorized users with a legitimate need for the development and administrative tools have access to them and extra precautions will be needed when using partitioned files. This management effort can be accomplished by assigning the primary responsibility of supporting the development efforts to some of the System Administration staff.

This SA responsibility includes the execution of the appropriate development tools to move the tested software into production, and the execution of the appropriate tools to establish a separate development environment to prevent contamination of the production environment. Another alternative is to restrict access of most development tools to supervisory-level development staff and disallow access to the remaining CDA staff. The use of Safeguard ACLs can reduce the management effort required to control a mixed system. For example, access to the development tools that are required infrequently may be frozen when not in use. In addition, to manage software revision control, access to software installation control/configuration management tools could be limited with ACLs to an authorized Production Control staff. This provides the additional capability to enforce controls over local programming or development and database structure or configuration changes.

- *Local policy will be established so the compilers and other development tools, on production only systems, are secured through file system security and access is restricted to only the SA group.*

- *Local policy will be established so that on mixed systems the compilers and development tools are secured through file system security, and access to these tools is restricted only to members of the SA group, the SSO group, and the CDA group on an as-needed basis.*

    - *A list of these compilers and development tools consists of at least the following, but is not limited to the following:*

BIND
C
COBOL
COBOL85
DEBUG
INSPECT
PASCAL
SCOBOL
SCOBOLX
SQLCI
SQLCOMP
TAL
TGAL

4.3 Auditing Security

When properly administered, Enscribe and Safeguard provide security for audit logfiles to ensure that only authorized users can access them. Tandem systems normally control and audit resources with the following facilities:

- TM/MP controls transaction-level data
- Event Management Service (EMS) controls hardware and event logs

Safeguard can be used to assist in controlling and auditing access to system objects for Kernel users, or to control and audit command-level access. The COTS BOSS product , audits user access, and controls command-level auditing (when the commands are executed through BOSS, only the fact the command was executed is audited).

NOTE: Currently there is no capability that exists to audit activity once a command is executed and until processing exits the command.

- *BOSS will be configured to audit all command-level and utility processing.*

4.3.1 Audit Strategy

The command-level users have access to system-level resources and therefore need to have the functions they perform audited. The application-level users have access to applications that could modify data, and therefore need to have the functions they perform audited. The database needs to be maintained in a state where data integrity is ensured; therefore, transaction-level data auditing is also required. The system could potentially have a hardware or software anomaly that could threaten the availability of the machine, or worse. Therefore, hardware and software anomalies also need to be audited and logged.

4.3.2 Audit Trails

Audit trails are required as a minimum to determine accountability, according to *DOD 8500.1*. They also provide the accountability functionality of a C2 level trusted requirement. This feature provides an investigative tool to detect misuse of the system and the gathered information has been used as evidence to convict individuals of computer crime.

Audit trails are required on all multi-user systems and must document the following information:

- The identity of each user having access
- The terminal the user is using
- The time of access
- The action being performed
- Any attempt to negate security
- Other security-related actions such as changing security levels

Audit Trail Maintenance needs to include the following.

- Review of audit trails is a function of the IAO or designee.

- Audit trails must be reviewed weekly at a minimum, but preferably daily, or as outlined in your local INFOCON Level Guidance, as long as it is not any less than weekly. Depending on the size of the system, the review can consist of the entire audit trail, a review of customized reports, or use of an automated audit-monitoring tool.

- Audit trail files must be protected by encryption, if possible. Access must be controlled to prevent unauthorized access, tampering, or loss.

- Audit trails must be maintained for one year in either paper or electronic form.

- Paper copies of audit trails should be treated as "FOR OFFICIAL USE ONLY" and shredded when no longer needed. Electronic copies must be cleared in some manner before disposal. For additional information, see the *DISA Computing Services Security Handbook, Section 3.5, Clearing, Purging, and Destruction of Material*.

- Audit trail reviews should focus on the following:

  - Unsuccessful logons
  - Changes of passwords
  - Use of equipment at questionable times
  - Questionable use of equipment, system functions, or applications looking for users who are (1) searching for passwords, (2) granting or stealing extra privileges, (3) scavenging disks, (4) browsing unauthorized files, and (5) uploading malicious code

4.3.3 Enable Enscribe Transaction Data Auditing

The TM/MP transaction-level data monitor/auditor ensures that data integrity is maintained to a data transaction level. This is accomplished by the application process executing a procedure call to BEGIN TRANSACTION when it is ready to start a logical transaction that updates, inserts, or deletes data from a database, and completes the logical transaction when the application executes the procedure call to END TRANSACTION. Also, if the transaction needs to be backed out, the application process can execute a procedure call to ABORT TRANSACTION. These commands can also be executed similarly in an interactive mode when a Database Administrator is accessing the database to perform database management with the SQLCI Data Base Management System (DBMS) tool.

When the TM/MP is notified to BEGIN TRANSACTION or END TRANSACTION, it captures before and after images of the data being modified to a transaction audit trail logfile. Periodically these audit trails fill up and require dumping to tape. When TM/MP is notified of the ABORT TRANSACTION, it replaces the modified transaction data in the database with the relevant **captured before** data images of that transaction data.

Additionally, the super-group members (SAs or System Operators), or a BOSS or Safeguard designated System Operator user, normally have the ability to recover a database to a consistent point in time by instructing TM/MP to roll forward or backout transactions. The system-level operators execute these commands through TMFCOM (the TM/MP command-level interface), which can notify TM/MP of the roll forward or backout transaction command requests. TM/MP then replaces the appropriate data stored in the production database with the captured before data images of the data modified. These before and after data images are stored in the audit trail logfiles and on-line data file dump tapes. See *Section 4.3.8, Protecting Audit Log Facilities*, for more information on TM/MP tape processing, and see *Section 6.3, Transaction Data-level Monitor (TM/MP),* for more information on transaction-level auditing.

The physical file size, the number of on-line audit trail files, the location of the audit trail files, and other configuration parameters need to be addressed prior to startup of application processing. These parameters are determined based on the amount of disk space available for audit trails, how frequently the audit trails can be dumped to tape, and the on-line roll forward or backout recovery required to support the operational production environment.

TM/MP has available reporting, data dumping, and transaction audit trail dumping tools (e.g., SNOOP). Additionally, third-party COTS software packages are available to assist in TM/MP management and audit trail evaluation.

- *The IAO, in conjunction with the SA, will ensure, at the local site level, that all Tandem systems have TM/MP appropriately installed, configured, and secured whether or not it is used.*

- *The IAO, in conjunction with the SA, will ensure that already existing production TM/MP capable databases, on the system, will be audited with TM/MP transaction data auditing prior to allowing any user-level access to the application.*

- *When there are databases on the system that are not TM/MP capable, the IAO, in conjunction with the SA, will document these databases.*

NOTE: The documenting of the database should include:

- Name and location of the database
- Owner and security settings of the database
- Sensitivity of the data in the database
- Operational reason for not auditing the database

- *The IAO, in conjunction with the SA, will ensure, at the local site level, that all newly installed production databases are audited with TM/MP transaction data auditing prior to allowing any user-level access to the application.*

NOTE: The Tandem IAO and SA will need to ensure the databases associated with the programs that contain the (BEGIN TRANSACTION, ABORT TRANSACTION and END TRANSACTION) procedure calls are audited with TM/MP.

4.3.4 Enable User Level Access Auditing with BOSS

The BOSS COTS product is a security access monitor that can control and audit user access on a Tandem system. The intent is to use BOSS to control and audit application users and TACL command-level user access. After BOSS is properly configured and started, it produces audit logfile data when users change their passwords, log on, log off, and access command-level utilities and applications. It also produces audit logfile data when updates are applied to the BOSS configuration database. The locations of these BOSS audit logfiles are configured in BOSS using the global environment screen.

The audit data that is logged by BOSS must be reviewed regularly in accordance with the *DISA Computing Services Security Handbook, Section 3.3*.

The reviewer must look for excessive numbers of failed logon attempts, excessive numbers of failed access attempts to applications or utilities, unauthorized access from other nodes, unauthorized access to system utilities, unauthorized configuration changes, and unauthorized password resets. The reviewer must carefully evaluate all access to SUPER.SUPER or SA userids to identify potential security breaches.

- *The IAO will ensure that the BOSS software has been installed to include modifying the local system startup obey file for starting the BOSS (e.g., $BOSS) during system startup and configured prior to allowing user access at the local site level.*

- *The IAO will ensure that the BOSS audit logfiles are reviewed in accordance with DISA requirements and local INFOCON Level Guidance.*

- *The BOSS audit logfiles will not be located on the $SYSTEM volume and will be located on the TM/MP audit trail volume or distributed across multiple volumes.*

NOTE: This will ensure there will not be a system performance problem due to the size and activity of the audit logfile.

- *The IAO will manage the audit data file rollover to ensure audit data is not lost.*

4.3.5 Enable Command-level Access Auditing with CMON

$CMON is a command-level access monitor that can control, monitor, and audit command-level user access to the standard Tandem system command-level interfaces (TACL and COMINT).

The SSO group will be the only group authorized to develop the CMON program, and the development will be done according to the Field Security Operations security specifications.

- *The IAO will ensure that the CMON software has been tailored for specific security concerns and user control at the local site level.*

- *The IAO or SA will ensure that the local system startup obey file (and CIIN command, if* *applicable) will be modified to include automatically starting $CMON during system startup by a command or by the obey file being executed from the CIIN file.*

4.3.6 EMS Considerations

EMS logs application and hardware events to a system event logfile. The system event logfile is located in the subvolume **$SYSTEM.ZZEVnn**, where **nn** is the octal number of the operating system image that is currently executing on the system. The EMS monitor and auditing software functions in conjunction with, and is complemented by, user (SSO) written EMS collectors, EMS filters, and report programs to manage the logging of events. Event messages can also be routed to other devices or processes for further alerts or action to be initiated. (For example, this could also include routing to network management software in the form of a standard Management Information Base [MIB] message.)

4.3.7 Protecting Audit Log Facilities

Activities on Tandem systems are audited with the following facilities:

- EMS for event logging
- TM/MP for transaction-level data
- CMON for command-level user access
- Safeguard for objects and command-level user access
- BOSS for user access logging

Potentially, the older Tandem systems may have a system-level event logfile facility $AOPR and OPRLOG that must also be addressed.

Protecting security audit log information is a multifaceted procedure. Security audit log information is not only included in the security monitor logfiles (BOSS, Safeguard TM/MP), but also in the system-level event log (EMS and OPRLOG) files. Each of these audit facilities has related files (i.e., obey, configuration, database, and audit logfiles), all of which will be secured and maintained to ensure the monitor tools are executed in a consistent and continuous basis. The initial Enscribe security will be set and properly administered to prevent unauthorized access or modification to the security audit information stored in these audit facilities.

The security audit logfiles will have reporting performed against them periodically. These reports need to be reviewed to determine if any security breaches have been attempted or accomplished in accordance with the *DISA Computing Services Security Handbook*, *Section 3.3*. Constant records of security-related information must be maintained. These logfiles need to be periodically rolled over to new logfiles, backed up so they can be recovered for later research or analysis, and then purged from the system to free up the disk space they are occupying.

- *The IAO will ensure that the audit facilities and related files are appropriately secured and maintained.*

- *The IAO will ensure that all the audit facility logfiles are reviewed in accordance with DISA requirements.*

NOTE: While reviewing the audit logfiles, some items to look for are as follows:

- Unsuccessful logons
- Changing of passwords
- Equipment or userids being used at questionable times
- Questionable use of system functions or applications
- Uploading or download files to and from the system
- A user browsing the system

Users that are attempting to use utilities they are not authorized to use

- *Audit logfiles will be periodically rolled to new logfiles, backed up to tape, and the old logfile purged from the system.*

- *Audit logfile backup tapes will be archived for a minimum of one year, offsite, unless otherwise specified as follows.*

NOTE: The following is the backup retention period for Audit logfiles.

TYPE OF AUDIT LOGFILES	RETENTION PERIOD
BOSS and CMON Audit logfiles	Keep for 1 year.
TM/MP Audit logfiles (Online dumps)	Keep for 6 Months.
TM/MP Audit logfiles (Transaction dumps)	Should be kept for at least 6 months of Online dumps. They should match up with the Online dumps.
All Other Audit logfiles	Keep for 1 year.

4.3.8 Enable Safeguard Object-level Auditing

Safeguard can be used as an object-level access monitor and audit facility to control command-level user access to Tandem system objects. If Safeguard is in use on your site, it is strongly recommended that object access be controlled using Safeguard ACLs.

4.3.9 Safeguard Audit Considerations

Safeguard maintains its related data in four groups of files. The configuration-related information is maintained in the following two files:

- $SYSTEM.SAFE.CONFIG
- $SYSTEM.SAFE.CONFIGA

The object-related information is stored in either the $<Volume>.SAFE.GUARD file for disk object types, or in the $SYSTEM.SAFE.OTHER file for all other object types. The subject-related information is maintained in the $SYSTEM.SYSTEM.USERID file.

The Safeguard audit log data files are sequentially created starting with number 0000001 through 9999999. The log data is maintained in the configured audit pool <$Volume>.<Subvolume>. If all configured audit pools fill up, log the audit to a default recovery area of $SYSTEM.SAFE.A0000001 through $SYSTEM.SAFE.A9999999 (but only on a limited access recovery basis). The SAFEART (Safeguard Audit Reduction Tool) product is for Safeguard audit logfile analysis and reporting.

If Safeguard is planned for use at the site, it is strongly recommended that care be taken while installing and enabling Safeguard to ensure that proper security is established prior to allowing any user access. Also to prevent security vulnerabilities, it is strongly recommended that care be taken to ensure the Safeguard database is properly secured, and audit data reporting is performed and reviewed regularly by authorized personnel.

4.4 Object Reuse

Kernel defines processing in two separate distinct states. These two states are privileged and non-privileged processes. The privileged processes can access the system areas as well as the user areas, and consist of operating system access and other high level, non-restricted access (these are considered to be part of the TCB). The non-privileged processes can only access the user areas and are restricted based on security permissions allowed for the user who started the process. Privileged processes do not go through the same security checks in Kernel and Safeguard as non-privileged processes.

The operating system software also enforces virtual-to-real memory mapping separation of the following six distinct logical areas of concern:

- User code (user program instruction pages)
- User data pages
- User library pages
- System code (system program instruction pages)
- System data pages
- System library pages

This virtual-to-real memory mapping ensures separation of individual process address space. The separation of user code, user data, user library, and system code, system data, system library virtual spaces is maintained by Kernel and virtually mapped to the Swap file on disk or the Program file on disk as secured through the standard File Management System software.

4.4.1 Memory Reuse

Memory or disk space once used (written to) and then released back to the system, cannot be reused without concern for data (information) being readable by other non-privileged users or user processes. The way Kernel and Safeguard address these concerns is described below.

The memory manager and operator process of Kernel ensures that memory used (written to by any non-privileged process, and once released by that process) cannot be retrieved by the same or by a different non-privileged user process. The only exception is in the case of an application using the ALLOCATE SEGMENT procedure call to lock memory, and then intentionally share the address of the mapped memory with another process via an inter-process message. The second process would need to be running in the same CPU as the originating process, and it would need to become active prior to the first process ending, or the locked memory by the first process would have been unlocked and the mapped memory released to the system. Therefore, the memory previously locked is unavailable for accessing through the non-privileged process, causing an instruction failure to the second process when attempting to access the address. The instruction failure causes the second process to ABEND with a trap.

4.4.2 Disk Space Reuse

The disk process, NSSQL database management system, and Enscribe file management system of Kernel ensure that data written to a disk volume by any user, once deleted, cannot be retrieved by normal operational processing and cannot be retrieved by a non-privileged user.

A file management flag (CLEARONPURGE) is available on each file in the Tandem system that can be turned on/off (provided one has appropriate access to that file) at any time in a file’s lifetime. If enabled, this flag provides an additional level of security and is available for sensitive data files. It ensures that when the data file is purged, the actual file is over-written with null values (HEX 00). Without this flag enabled, the disk volume file label information is only logically marked as deleted.

- *The IAO will maintain a list of all files containing sensitive data and will ensure the CLEARONPURGE bit has been set to include, but is not limited to the following files:*

  BOSSID2
  USERID

4.4.3 Application Process Reuse (Context Free Servers)

There are special considerations that CDA personnel will apply during application development to ensure a server process does not retain requester data from one client (after replying to that client) and allow the data to be incorrectly applied to another client's request. The server programs need to be developed as context free servers. The requester/client processes need to retain sufficient relevant information to support a user's successive requests to the same server class, passing all the required information in an inter-process communications message to the server process along with the server request. The client processes also need to be coded so that each successive user of a client starts out with the same lack of information as the previous client user.

The Tandem Inspect tool assists in program debugging. This tool can interactively access object program variables to display parameters and program source code for developers. While this is helpful in debugging programs, it poses a potential security risk, which could easily be avoided. The Inspect symbols must be removed prior to putting the programs into production. For further information on how to check for these debugging parameters and applying this fix, see the section entitled, How to remove the INSPECT debugging tool parameters stored with an object program, in *Appendix D, "How to" Guide for Tandem (NSK).*"

- *The IAO and the SA will test the applications software programs to determine if privileged code is being used by:*

  - *Attempting to execute the program in a test environment under a non-privileged userid (not SUPER.SUPER), or,*

  - *Using the FUP tool to check for the license flag being set.*

  - *Also using the BIND and NOFT in Section D ("How to check for privileged programs").*

- *When a program contains privileged code, the IAO and the SA will maintain a list of all privileged code programs for each application and take the appropriate action to verify the DISA Computing Services (formerly DISA WESTHEM) or the DISA Computing Services CCB has issued approval for this program to exist on the system.*

- *When the program contains privileged code and has not been approved, it will be secured away from use, and treated as a high-risk vulnerability with the potential of seriously compromising system security, until the program is approved for use.*

- *The SA will ensure object (program) reuse is being implemented at the application level by accessing the applications programs (from more than one (client) device simultaneously, from one or multiple application userids, or from multiple similar consecutive accesses) to ensure there is no residual information in the presentation to the clients.*

NOTE: The reuse of the application programs will aid the software module update process. If the software module is not reused, then the SA would have to duplicate the software object module according to the number of clients. There should also be a concern about the disk drive space that multiple copies of the same software module would require.

- *The SA will test each of the applications software programs by using the BIND utility to determine if the program's symbols have been removed.*

- *The SA will document all programs containing symbols with the IAO and will ensure that the responsible CDA is notified*.

5. TANDEM SYSTEM INTEGRITY

The sites achieve Tandem system integrity by managing the overall processing environment. Proper security and system management protects hardware, operating system software, applications, data, and standard system configurations from unauthorized access or improper modification and leads to the secure operation of Tandem systems as a TCB. To ensure proper execution, it is important to control the operating system image revisions and configuration. The integrity issues can be grouped into two areas—hardware integrity and system integrity.

5.1 Hardware Integrity

Every operating environment is composed of hardware resources. These include elements such as the CPUs, direct access storage devices (disk drives), disk volumes, tape drives, tapes, consoles, hard-copy logs, printers, terminals, and communications devices.

When handled improperly, these components can create exposures within the operating environment that cannot be controlled with any software process.

- The CPU could be *halted* from the OSP/RMI (Operations and Service Processor/Remote Maintenance Interface) system console, the memory in that CPU could then be dumped and the data that is stored in memory could be accessed.

- A disk volume can be accessed via a physical level diagnostic and maintenance tool (e.g., TMDS or TANDUMP), the data stored on the disk could be dumped to a screen, modified, and written back to disk. If access to this facility is not restricted, the exposure exists that data could be altered. This could result in corrupted information or access to data without proper authorization.

- Equipment manufacturers and service technicians generally have facilities that allow local OSP/RMI, and/or remote dial-up access to service facility so diagnostics can be run if equipment problems occur. The system availability could be jeopardized, and the data can potentially be accessed, modified, and/or destroyed by personnel who are not qualified or who cannot be trusted to perform such diagnostics.

The system hardware console OSP/RMI has full command-level accesses on it. This device will be located in a controlled access area, and will only be accessible by authorized personnel.

Tandem hardware provides for a level of fault-tolerance for all critical system devices (i.e., CPUs, I/O controllers, disk drives, disk volumes, communications ports, etc.). This fault-tolerance provides added reliability to ensure the necessary production functions are accomplished even if a single point of hardware or software failure occurs.

Please note that mirrored disk volumes are two identical copies of the data stored on two separate physical disk drive volumes with both packs being treated as halves of the single logical disk volume. Also, note that to recover to the live-mirrored state after a new physical disk volume is installed only requires that a utility command be executed, and the new mirror backup disk volume will be synchronized with the data from the live production half. Again, there are two physical copies of the data available to the system, maintained as one logical copy.

Spooler output (printed reports, reports on microfiche, reports on compact disk, reports on floppy diskettes, etc.) presents a significant exposure if the information is not handled in accordance with applicable regulations. The information on output media will be properly safeguarded. The users will have on file the appropriate SLA before data output is authorized. This also addresses the need to control access to all removable media.

Data being downloaded to a client’s Personal Computer (PC) needs to be treated with the same level of security classification as existed on the Tandem for that data. The client user is responsible for the data on their PC and they will ensure the appropriate security measures are taken for the stored data. The site, in conjunction with the data owner, might consider having an MOA or SLA on file before the client user is allowed to download data to that user’s PC.

This STIG is not intended to address client security. Refer to the *Network Infrastructure STIG*, the *NSA NT Guide*, and the *DISA NT Addendum* for more information in this area.

In addition, this document is not intended to address the resolution of the integrity of the hardware environment. Access controls will be designed and implemented as part of the physical security plan for the site. The concept of I&A is the principal mechanism for controlling these resources. One example of such a process is a card key system that provides both identification and a code number for authentication.

DISAI 630-230-19 and the *DISA Computing Services Security Handbook, Section 3.0*, provide further guidance on the proper protection of the physical environment.

- *The IAO will ensure that the access to special maintenance tools (e.g., TMDS, TANDUMP, DIVER, and RELOAD) is controlled so only the SA group has access to them.*

- *The IAO will ensure that all TCBs, including the OSP/RMI, will be located in a secure controlled access facility area.*

- *The IAO will ensure that local policy is in place to address the proper handling of removable data and reports.*

NOTE: The following are an example of removable data and reports:

- Backup tapes
- Data tapes
- Floppy disks
- Reports
- Hardcopy

Data sent over the communications network.

5.2 System Integrity (Operating System Software)

Integrity of the operating system software environment consists of securing the system configuration, the system-level processes, and the data-level processes. The operating system software consists of the following groups of components:

- Kernel (including the message system, operator process, monitor process, dispatcher process, memory manager process, and the interrupt handlers)
- TM/MP
- Safeguard
- Enscribe
- NSSQL DBMS
- I/O processes
- Event Management Service
- System procedures

The CONFTEXT (configuration input file), Installs database, the Distribution Subvolumes (DSVs), the Installation Subvolumes (ISVs), the operating system software release bundle, and related compatible IPMs are all stored on the disk volumes as files requiring the same type of safeguarding as other critical database files. Installs database, DSVs, ISVs, the operating system software release bundle, and related compatible IPMs will be owned by the SA userid, and will be secured so other users do not have access to them. The CONFTEXT file must also be owned by the SA userid. However, *read only* access to other users in the System Administration group may be permitted.

System configuration integrity is ensured with the Install system configuration software tool.

Install reads the CONFTEXT (configuration input file) and verifies the information in its database with the existence of the DSVs, the ISVs, the operating system software release bundle, or compatible IPMs. After Install has verified the configuration, hardware, and software options are compatible with the operating system software, it attempts to bind into a single operating system image by initiating the SYSGEN process. SYSGEN creates a new operating system image after it verifies the hardware configuration parameters are compatible.

If a change is needed to the system and time does not allow for a SYSGEN, the Tandem supports dynamic modification of the system configuration using the COUP (Configuration Utility Program) and DSC (Dynamic System Configuration) tools. Anyone making dynamic changes to the Tandem must exercise caution when using the dynamic system configuration tools for the following reasons:

1. The changes made to the system configuration are made against (bound into) the executing copy of the operating system image and are lost when the operating system is rebooted for any reason. The changes must be reapplied to the executing copy of the system image after the system is rebooted. Therefore, a record of the changes must be kept in case they are required.

2. Complete system configuration integrity is not assured (to the degree it would be) when using Install. Problems can occur that would normally be flagged in the SYSGEN verifications.

3. No record of changes is maintained when using DSC and/or COUP if the **LOG** command, to create an audit of the commands entered while using this tool, is not enabled.

4. Unpredictable results could occur if, while modifying the system configuration with COUP/DSC, the CPU or system where the COUP/DSC tool is executing crashes, or if the COUP/DSC process hangs or aborts.

System-level (machine configuration management) integrity consists of protecting hardware and software resources from unauthorized access and modification. Kernel was developed from a modular design, with fault-tolerant (NonStop) processing, and each process was designed to be a multi-threaded process. The modular software design lends itself to prevention from attack where the system-level processes would ABEND and the exposure would exist for another process taking over a system-level function. With the top-down structured programming design to prevent data and code stacks from filling up, client/servers processes are intended to run forever or until instructed to cease execution by a standard procedure (i.e., normal end of file).

System configuration on Tandem systems requires the generation of an executable operating system image. This is accomplished by compiling a specific set of hardware descriptive configuration parameters, hardware drivers, interrupt handlers, and the Kernel software, then binding these into an executable operating system image. It is critical to have the corresponding operating system image to match the current standard system configuration or the system cannot function as desired. Care needs to be taken to provide change control of operating system image configurations.

Data-level integrity consists of protecting database hardware resources and software resources from unauthorized access and modification. In addition, maintaining the availability of the database to the user is part of data-level integrity.

To ensure system integrity, changes to critical system and data files must be controlled and monitored. The concept is to first verify the system critical items are in the appropriate state for secure operations. Following this verification, create a baseline that documents the current state of all the critical items. Maintain an authorized changes database that documents the changes that were authorized. Periodically compare the current state of the critical items with the defined baseline. Note the discrepancies and compare them to the authorized changes database. Take appropriate action when unauthorized change discrepancies exist. These comparisons verify the system-critical items are in the appropriate state for secure operations. Periodically a new baseline should be created after the current state of system integrity has been assured. This serves to incorporate authorized changes into the baseline and minimize the authorized changes database.

Reviewing the following items helps to assure that only authorized changes have been introduced into the system:

1. The database (physical and logical distribution, data file structures, data population, catalogs, views, etc.)

2. The operating system software (SYSnn subvolume, system subvolume, and other related subvolumes)

3. The system configuration (DSV, ISV, customer subvolume, and Install database)

4. The Pathway configurations

5. The application object programs

6. The application source code

7. The communications connections (Local Area Network [LAN], Wide Area Network (WAN), EXPAND, direct connects, etc.)

8. The job batch scheduler configuration and workload

9. The processes executing on the system

10. The system workload balance

11. The TM/MP system (configuration and library)

12. The tape management software (configuration and library)

13. The security tools and audit logfiles are intact.

- *The IAO will ensure that the installation files and related configuration files are properly secured so only the System Administration group can access them.*

- *The IAO will ensure that the operating system and related files are properly secured so only the System Administration group can modify them.*

NOTE: The files that comprise the operating system and related files may vary from site to site due to operating systems differences (e.g., D39, D48, Safeguard, etc.). Please refer to the Tandem (SUT) documentation for more information.

- *The SA will maintain a current drawing of the physical hardware configuration.*

- *The SA will maintain a current drawing of the logical (MACKIE) hardware configuration diagram.*

5.3 Pathway Application Configuration Management Integrity

Pathway is the applications software management facility that runs on Tandem systems. A monitor program called PATHMON manages the Pathway applications software management facility. Pathway has three main groups of resources that are managed under PATHMON:

- Servers
- TCP (Terminal Control Processes) (sometimes referred to as client requesters)
- User terminals

PATHMON and all the processes it manages can be configured to execute in a NonStop fashion, with supporting TM/MP data transaction auditing. Pathway is configured as owned and managed under a specific Kernel userid, to execute in specific CPUs, at specific priorities, with specific devices assigned. Pathway supports pre-defined static as well as dynamic configuration of the applications, maintains application servers, TCPs, and terminals configurations, manages the multi-threading of, and handles the link management between, the TCP and the server processes. Pathway is configured to manage the related servers, TCPs, and terminals as a group of objects to support a specific application system or subsystems.

- *The IAO will ensure that the Pathway configuration and related files are properly secured so only the System Administration group can modify them.*

- *The IAO will ensure that the Pathway system is configured properly to provide secure applications access.*

5.4 Data Integrity

Data integrity consists of protecting the database structures (physical and logical databases), the data integrity, Enscribe file security, data accessibility, data reliability, and data transaction integrity. Included in data integrity is the assurance that logic design rules are followed in the database management, and that control is exercised over the data views (e.g., protected view) to provide secure access to the data as required by the users.

5.4.1 Database Structures

Tandem's NSSQL database management software ensures structure, physical layout, catalog owners, tables, views, and database rules (e.g., if an element X in the column Y is greater than a specific value, then allow access to specific rows; otherwise no access is allowed). Another implementation is that of protected views that allow users access to only a subset of rows to be observed in a table, or a subset of rows from multiple joined tables. These are maintained by NSSQL, and enforced when users attempt access to the data in the SQL database.

5.4.2 Enscribe File Integrity

Tandem's Enscribe security ensures the disk file owner and access security parameter values are checked against the Kernel user's access privileges (that are retained in the PAID and CAID settings of the user's process) prior to granting access to the data files. This allows or disallows access to the resource. More information related to file security parameters will be found in *Section 4.2.4, Default Users File Security Settings*.

- *The IAO will ensure that the appropriate Enscribe and NSSQL database security is set and maintained on all database files, database tables and related application supporting files.*

NOTE: Related application supporting files are as follows:

- Configuration
- Programs
- TACL macros
- Obey files
- DDL files
- SQL catalogs
- Object program files
- Libraries

Related source files

5.5 Data Accessibility

Data accessibility is ensured by Kernel maintaining the availability of the resource through use of fault-tolerant hardware design, software design (e.g., I/O processes are modular, NonStop, and many [such as the disk process] are multi-threaded to enhance performance). The DP2 disk process part of Kernel is the I/O software process that is used to access the disk resources. The disk controllers and disk drives hardware are a dual-ported design to provide fault tolerance and ensure the maximum level of availability possible. Response time is also a critical factor in the appearance to the user of data accessibility and availability. This can be enhanced with proper database design, implementation, maintenance, and periodic database tuning that need to be reevaluated on a regularly scheduled basis.

5.5.1 Tandem Disk Controllers

Tandem disk controllers are dual-ported and multi-attached to a pair of CPUs. The disk controllers can be physically accessed from either CPU to which it is attached. Therefore, data stored on disk drives is directly accessible from either CPU attached to the dual-ported disk controllers.

5.5.2 Tandem Disk Drives

Tandem disk drives are dual-ported and multi-attached to a pair of disk controllers. The disk drives can be physically accessed from either attached disk controller. Therefore, data stored on disk drives is directly accessible from either disk controller attached to the dual-ported disk drives.

5.5.3 Tandem Disk Volumes

Tandem disk volumes can be configured as a mirrored pair, and logically addressed as a single unit or volume. Data reliability is ensured through disk mirroring because the data is written to both halves of the mirrored pair simultaneously. One of the advantages to mirrored volumes is the data can be read off either the primary volume or the mirror volume. If one side of the mirrored volume becomes corrupt or inaccessible, and the data is not corrupted on the other side of the mirrored volume, the system automatically completes the request for the authorized data needed.

In addition, if one half of a mirrored pair needs to be replaced, it can be performed while the other half remains on-line to the users. The replacement half of the mirrored volume can be re-mirrored to the original live production half quickly and easily by a system operator with the execution of a single PUP (Peripheral Utility Program) tool command. Therefore, data stored on disk drives is directly accessible from either CPU attached to the dual-ported disk controller; either disk controller attached to the dual-ported disk drives and from either half of the mirrored (pair) logical volume. For performance as well as fault tolerance, all disk volumes must be mirrored. Exception requests should be addressed to DISA Field Security Operations.

- *The IAO will ensure that the operating system image volume $SYSTEM and all critical production data volumes are mirrored.*

NOTE: Optical drives are the exception to the required mirrored volumes.

5.6 Database Reliability

Kernel has several features that ensure the data in the database is reliable, and only authorized processes and authorized users have access to the data. There are several tools to assist in data management. Data management includes two layers of management:

- Physical device (disk drive, disk volume, location)
- Logical database (file, table, row, column, transaction, and backup copy)

File management, database management, transaction management, and system management all play an inter-woven and important part in database reliability. Several tools have been developed by Tandem. Some of these tools cross the physical/logical and hardware/software management boundaries.

The only authorized access to a database or file for an application user is through a pre-defined and pre-tested application interface. The only command-level user access of data management tools on a *production only* system will be for the System Administration group, and then only as needed for database maintenance, disk volume maintenance, hardware maintenance, operating system software maintenance, and tuning. The command-level user access of data management tools on a *mixed* system will be restricted to the System Administration group and then only as needed for database maintenance, disk volume maintenance, hardware maintenance, operating system software maintenance, and tuning. There is an exception for command-level user access of data management tools on a mixed system where the SSO group and CDA group must also have access to these tools for testing, but their access will be restricted to only the non-production databases, except as noted in *Section 4.2.7.1, Database and File Management Access Tools*.

- *The IAO will ensure that all application user access is through the Pathway applications interface.*

- *The IAO will ensure that all database management tools accessed by application users are limited and controlled, if possible, through similar application tools.*

These database management tools will include but are not limited to the following:

- SQL statements
  - Data Definition Language (DDL)
  - Data Manipulation Language (DML)
  - Data Command Language (DCL)
  - Data Status Language (DSL)

- SQL utilities

- Guardian utilities
  - BACKUP
  - DSAP
  - FILCHECK
  - FUP
  - MEASURE PRODUCT
  - PERUSE
  - PUP
  - RESTORE
  - SAFEGUARD PRODUCT
  - TACL
  - TEDIT
  - EDIT
  - VIEWSYS

Figure 5-1: Database Management Tools

- *The IAO will ensure that transaction auditing is used for all critical data files to ensure audit logging and recoverability.*

***NOTE**:* Critical data files are files such as but not limited to the following:
- Operating system files
- Configuration files
- Databases
- Some application files

NOTE: See also *Section 4.2.6, Object Access Controls.*

- *The IAO will ensure that these database management tools will only be accessible on an as-needed basis to System Administration group users.*

See *Figure 5-1* for a list of the database management tools.

- *The IAO will ensure a local procedure is established and followed by the IAO or the SA to verify the database integrity at least weekly after the file management, database management, transaction management, tape management, and system management tools are used.*

NOTE: "DSAP *, BROKEN" can be used.

> This command will list all of the corrupted files on the specified volume. If you use * for the volume instead of the volume name (e.g. $SYSTEM), all the drives on the system and the corrupted files on each drive will be displayed.

The IAO will need to use the corrupted file list in order to correct the corruption in the files before anyone or any application reads or writes data to that database. If the corrupted file is not corrected before reading or writing data, corruption, the data read or data written my be corrupted and not recoverable.

- *The IAO will ensure that access to database catalogs and file structures is controlled through DAC and limited to the administrator in the appropriate Administration group(s).*

- *The IAO will ensure that access to the tape management software and tape library is controlled through DAC and limited to users in the System Administration group.*

- *The IAO will ensure that all SQL database access for application users is limited to and controlled through table views as defined by the appropriate Administration group in conjunction with the CDA.*

5.6.1 Database Management System Security

Access to production databases, catalogs, and file structures will be limited (via DAC) only to users in the System Administration group. This can include controlled access down to the level of columns and elements in those columns. Access to file management system tools (e.g., FUP, DDL, Enable, Encore), database management tools (e.g., SQLCI), and 4th Generation Language (4GL) database access tools (e.g., FOCUS), will be allowed only to the System Administration users group with respect to the production databases.

Access to file management system tools, database management tools and 4GL database access tools can be allowed for SSO group and CDA group users on an as-needed basis if these users are restricted to using these tools against only non-production database, catalogs, and file structures, except as noted in *Section 4.2.7.1, Database and File Management Access Tools*. All other users must be restricted from accessing these tools directly and indirectly through the application system software. NSSQL database tables have access to data controlled through SQL views and SQL rules as pre-defined by the DBA (Database Administrator) and the SA.

5.6.2 Labeled Tape Processing and Tape Management Software

Labeled tape processing can be enabled on the system to increase the conscious effort by everyone involved in tape handling, and to ensure the programs use the correct tape. In addition, a tape management software package needs to be active to provide the needed management of the tapes and to ensure tape retention and processing requirements are followed properly.

Using an on-line tape management software system aids in quick cross-reference of physical tapes to the data they store, which can speed recovery of databases when necessary. External labeling conventions for data stored on the tapes will be standardized to assist in the prevention of tape mishandling and the undesired destruction of data.

- *The SA will ensure a local procedure is established to address the regularly scheduled maintenance of tapes in the tape library to include the use of labeled tapes (e.g., internal labels, external description, and external numbering).*

5.6.3 File and Database Backup and Recovery

File backup and recovery is an important part of data reliability. Data is normally stored in tables and files on disk and/or tape. While the data stored on these disks and tapes is readily available and reliable, it could be inadvertently modified due to user error or other reasons. Therefore, for recoverability reasons the data will periodically be backed up. Without data backup, recovery of information is extremely difficult, and may need to be manually re-entered into the file/DB.

For further details regarding backup and recovery, refer to *Section 9, Tandem System Backups.*

Enscribe access security is not available for tape volumes or tape files. Therefore it is imperative the Enscribe file security be set on the system tools (e.g., Backup, Restore, FUP, etc.) that control tape processing. However, tape drive access security may be addressed by using Safeguard ACLs to limit user access to the tape devices. The use of Safeguard (if available on the system) to control security for tape drives is strongly suggested.

- *The IAO will ensure that a local procedure addresses tape-handling security because Tandem Enscribe security does not apply to tape volumes.*

- *The IAO, in conjunction with the SA, will ensure that local procedures address regular database backups.*

- *The IAO will ensure that the file system security prevents unauthorized access to system tape processing tools.*

6. TANDEM SYSTEM SECURITY MANAGEMENT

System-level access and integrity control will be maintained. The use of software monitoring and auditing tools to track the user's activity on the system, followed by IAO analysis of user activity reports is the best way to complete the security management task. This section defines the resources that assist the IAO and the SA to manage security on the Tandem systems.

6.1 Tandem System Modifications and Enhancements

DISA Computing Services establishes approved configurations and the policies and procedures for any configuration changes.

- *The IAO will enforce procedures to ensure that all system modifications and enhancements are in accordance with the local Configuration Control Board (CCB).*

6.2 Command-level Access Security Monitoring

BOSS is a COTS security software monitoring and auditing tool capable of controlling command-level user access. BOSS will be used to ensure command-level user conformance to security in accordance with the *Computing Services Security Handbook* for the majority of command-level user access. There are a few exceptions (mentioned previously in *Section 3.3.4, Non-BOSS TACL Access*) where BOSS will not perform the command-level access security. In these exceptions, the CMON and, if available, the Safeguard tools, will perform the security functions for the command-level user access. The assignment of only one groupnumber to one groupname, and one usernumber to one username, will be strictly adhered to when defining command-level users.

NOTE: BOSS does not validate the uniqueness within groupname, username, and groupnumber, usernumber. Special care should be taken to avoid duplication. Kernel does report an error in the EMS logfile, but it is not currently detected by the BOSS application. If duplication occurs, it will be in the BOSS database only.

- *The IAO and the SA will ensure that BOSS is configured to provide the required level of auditing, monitoring, and security management of command-level access.*

- *The assignment of only one groupnumber to one groupname, and one usernumber to one username, will be strictly adhered to when defining command-level users.*

6.3 Transaction Data-level Monitor (TM/MP)

TM/MP is a data transaction-level auditing tool that assists in data integrity assurance. If the servers accessing the database are written with TM/MP code, then auditing is enabled by turning on the file management flag on each database table or file. Once the flag is turned on, the TM/MP software ensures the data in this table or file is consistent to a transaction-level integrity across the database as directed by the **BEGIN TRANSACTION**, **END TRANSACTION**, and **ABORT TRANSACTION** commands. This also provides a transaction-level data backout and roll forward facility for those tables or files. Transaction-level data monitoring will be done for critical production databases. TM/MP ensures data integrity through a record-locking protocol that prevents concurrent updates from occurring to the same record(s) in a database.

TMFCOM has some reports available to display the current status of the on-line dumps that TM/MP is auditing and the status of all tape media being included in the TM/MP audit facility. The IAO must verify the on-line dump history includes the standard number of revisions. Also, the IAO must verify the tape media catalog is currently sufficient to support TM/MP file dumping requirements and is being maintained properly.

- *The IAO or SA will ensure that TM/MP capable production databases are audited by TM/MP.*

- *The TM/MP reports will be reviewed on a regularly scheduled basis.*

- *The IAO and the SA will ensure that TM/MP is configured to perform secure transaction-level data auditing of TM/MP capable production databases, and will ensure transaction-level integrity for updates being applied against TM/MP capable production database files and tables.*

6.4 Monitoring Applications and Related User Access

Applications can be defined (configured) and managed through the Tandem standard application management tool Pathway. BOSS must be used to control, monitor, and audit application-level user access, to analyze potential security risks, to assist in management of resource utilization, and to assist in recovery from any security breach.

6.4.1 Application-level Users and Software Monitoring Tools

Application-level user activity must be monitored and audited. The IAO must manage access to all the terminals that are defined for application-level user access, the database application software access, and the programs that are executed by the application-level user from within the application subsystems. The IAO or the Domain Manager must manage the user's access to the required applications and functions.

To perform application auditing within BOSS, it must be configured with the appropriate parameter settings. After the global BOSS parameters have been set, further specific configuration issues must be defined in BOSS. Users are defined in BOSS using user file records. Applications are defined in BOSS using **Application Information** records. Once the applications are defined in BOSS, functional groupings can be defined in related profile records. Access to application functions can then be defined by using **MenuInfo** records. The user access to an application is defined in BOSS by linking **MenuInfo** records to users or groups of users.

- *The IAO will ensure that application-level user access (database access and programs executed) is controlled, monitored, and audited.*

- *The IAO or the Domain Manager will ensure that the assignment of only one groupname and one username will be strictly adhered to when defining application-level users.*

- *The IAO may delegate a portion of these responsibilities to the TASO. However, the IAO has ultimate responsibility.*

6.4.2 Pathway On-line Application Multi-thread Monitor

Pathway will be configured to manage and monitor the terminals that are defined for the application-level user access, TCPs, server classes and the processes to which the application software user requires access. Periodically, the IAO will verify the Pathway configuration and startup obey files are consistent with the live production Pathway system executing at the site.

- *The IAO and the SA will ensure that Pathway is configured and maintained to monitor and manage application-level user access.*

6.4.3 Batch Scheduler and Monitor

When used, a batch job scheduler and monitor like NetBatch will be configured by the IAO and the SA to manage and monitor the application-level user's batch jobs that are accessed through standard Pathway server calls to queue batch jobs.

- *When the batch job scheduler is in use, the monitor software configuration and the startup obey-files will be periodically verified for consistency with the live production system executing at the site.*

- *When used, the batch job scheduler and the monitor will be configured and maintained to monitor and manage application-level user batch jobs.*

6.4.4 Maintaining Satisfactory Performance

System performance monitoring and tuning can be important to ensure security problems do not arise due to a delay in processing by the security monitor or audit log functions. Security software delays can inhibit attempted workarounds, and therefore may be disabled or bypassed in an attempt to allow sufficient resources to accomplish the main mission. Regular system tuning can ensure satisfactory transaction response time for the users, minimize delay, optimize resources, and assist in maximum utilization of resources.

6.5 Safeguard Object-level Access Monitoring

The Safeguard security tool may be configured and used to help manage object-level access security for monitoring, controlling, and auditing user activity. Security-related access reports can be generated with the SAFEART tool. These reports could be used to aid in the detection of unauthorized user object access attempts (successful or unsuccessful). Regular review and analysis of all security reports are critical in prompt detection of unauthorized access, either attempted or successful.

If the Safeguard tool is in use at the local sites, it is imperative to appropriately configure Safeguard to aid in the auditing of user activity relative to the monitoring, controlling, and security management of objects. It is also imperative to review the audit data on a regular basis. SAFEART is the audit reduction tool available for evaluating and generating audit reports from the Safeguard audit data.

7. RECOVERY FROM A SYSTEM COMPROMISE/ALTERATION

If there is a suspected attack on a Tandem system, the SA must take immediate action to stop the attack and gather the needed information to determine what, if anything needs to be restored.

NOTE: If the SA starts to restore information without knowing the full scope of the attack then the restore process may cause updates to be lost. This loss of information would be for files, which were updated since the backup that is being used to restore the information back to the system.

After the SA has completed the investigation and the suspected attack is deemed as being an attack, the SA will then start recovery procedures. The objectives of recovery from a Tandem system attack are containment, damage assessment, recovery, and correction of the security vulnerabilities.

NOTE: An on site SOP (Standard Operating Procedure) must be in place to detail how the recovery objectives are to be accomplished.

7.1 Identification and Notification

The identification and notification step of recovery includes the following procedures that will be executed when the security policy of a Tandem system is violated.

- *The IAO will customize the sample procedures to meet the local site needs for identification and notification as follows:*

  - *For logging and reporting all events related to an attack, incident, or natural event*

  - *For identifying whether the event, incident, or attack is real. (Determine if an incident did in fact occur or not.) If it did occur, perform the on-site SOP system compromise recovery procedures.*

NOTE: These procedures will contain instructions for performing a full disk dump (not file dump) of the affected hard drives. The disk dump may be supplied to the proper authorities.

  - *For notifying the proper authorities in the chain of command if an incident or attack is confirmed*

  - *For identifying who will be notified internally if a security policy violation is suspected or confirmed*

  - *For identifying the authorities to be notified when a Tandem operating system has been violated or is suspected of being violated*

7.2 Containment

The next step in recovery from a security policy violation is containment. Containment is designed to limit the extent of an incident. An essential part of containment is determining whether or not to shut down the system. The procedures listed below will be executed next.

- *The IAO will develop procedures for containment as follows:*

  - *For logging all events related to containing an incident*

  - *For determining if an incident/attack has compromised the system's integrity*

  - *For determining how the system must be isolated from the network or if isolating the system from the network will cause the any programs on the system to delete itself. (This procedure must include such steps as severing all communications connections, stopping all user processes, shutting down Pathway and all other applications, shutting down Spooler and other operating system processes, and perform a full system dump before shutting down the system. Evidence maybe destroyed.)*

  - *For properly handling any suspicious files*

  - *For notification to users of the anticipated outage*

7.3 Eradication

The next step in recovery from a compromise is eradication. The cause of an incident/attack must be eradicated once it has been detected and contained. If the cause of the violation is not fully removed from the Tandem system, it could recur in the system. The procedures listed below will be executed next.

- *The IAO will develop procedures for eradication as follows:*

  - *For logging all actions related to eradicating residual components of an incident/attack*

  - *For preserving corrupted or bogus files or programs for future analysis*

  - *For backing up and maintaining bogus files and programs for future analysis*

  - *For ensuring system backups are not corrupted*

  - *For eliminating the origin of an incident/attack when possible*

  - *For ensuring all programs on the system are authorized*

  - *For incident reporting*

7.4 Recovery

Once the cause of an attack has been contained and eradicated, the system must be recovered. The Tandem system offers automatic hardware recovery for all hardware that is configured as fault tolerant, and in the event, of a single fault failure, continuous processing for the task is accomplished by re-routing the work. Kernel runs NonStop, which offers automatic recovery of system-level functions. Kernel also allows the NonStop processing of application software and provides the same automatic recovery of application processes. Non-privileged applications programs cannot modify the operating system; however privileged applications programs can. Therefore, hardware and Kernel recovery (depending on whether or not privileged applications are allowed) is probably not required. However, database and application software may need to be recovered.

- *The IAO will develop procedures for recovery as follows:*

  - *For logging and reporting all events related to recovering from an attack*

  - *For removing known bogus files or programs and documenting the proper authorities that directed the file removal(s)*

  - *For restoring any or all parts of the system and verification of the system as necessary depending on the extent of the attack*

  - *For resumption of production processing*

  - *For notifying users of the need to recover to a specific point in time due to system compromise*

  - *For recovery of the database to a consistent transaction-level state*

  - *For asking the users to reapply any transactions between recovery point in time and the state of the database prior to recovery*

7.5 Attack on System Administration Account

- *The IAO will develop procedures for handling a violation (or a suspected violation) of an SA account (normally the SUPER.SUPER userid) as follows:*

  - *For logging and reporting all events related to an incident/attack on an SA account*
  - *For immediately notifying the proper authorities*
  - *For immediately isolating the Tandem system from all networks*
  - *For system recovery*
  - *For checking operating system image and configuration files*
  - *For changing all passwords on all accounts*
  - *For downloading audit logs*
  - *For standard recovery*

7.6 System Cleansing

- *The IAO will develop procedures for handling the clean up after a violation (or a suspected violation) of the affected software and data files as follows:*

  - *For logging all events related to clean-up*
  - *For immediately notifying the proper authorities*
  - *For backup of affected (attacked) software and data files*
  - *For identification of the entry point*

7.7 Closing the Loophole

- *The IAO or TASO will develop procedures for prevention of further incidents/attacks once the entry point has been identified.*

  - *For analysis of all events related to the violation and clean-up*
  - *For immediately notifying the proper authorities regarding patches, if required*
  - *For design, development, and testing of a lock (patch) for the access point*
  - *For implementing the access point lock (patch)*

8. TANDEM SYSTEM NETWORK COMMUNICATIONS

Figure 8-1 below shows all the connection types for the Tandem. These connection types will be discussed throughout this section.

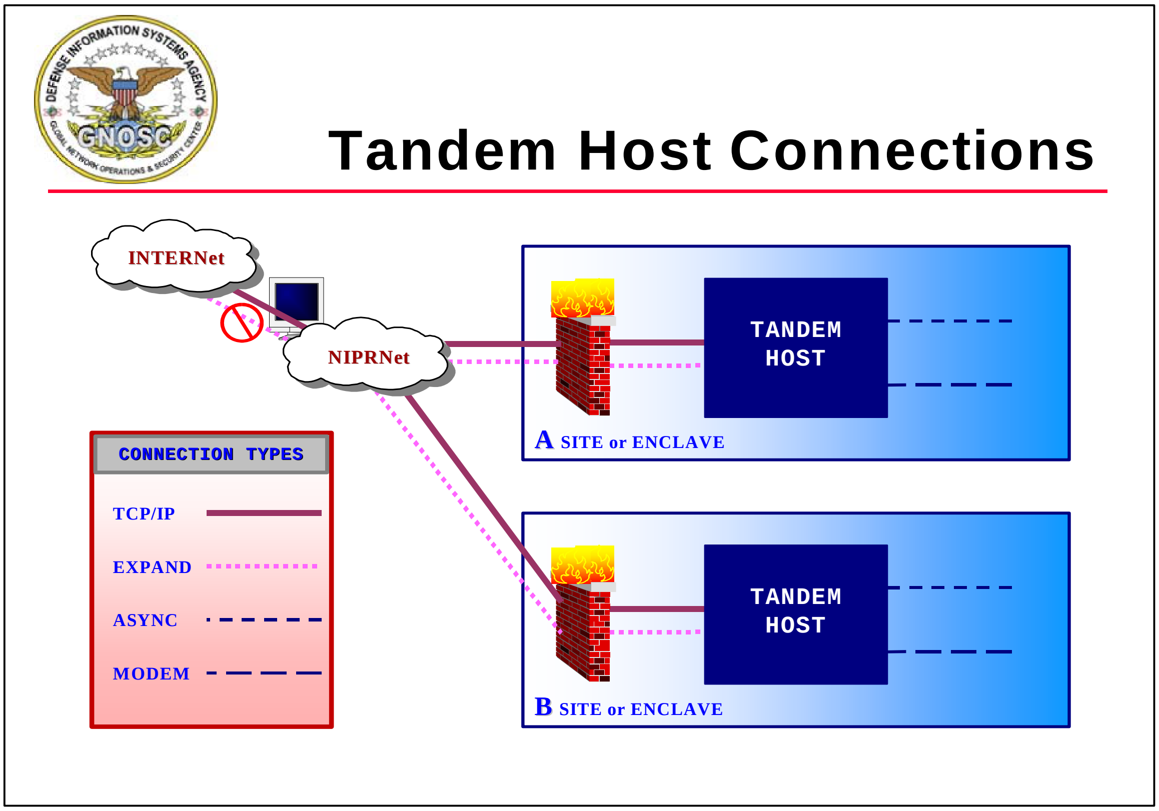


Figure 8-1: Tandem Host Connections

Network connections, as related to the Tandem systems, address the open system access side of the Tandem systems environment and consist of the following five scenarios:

- Tandem to Tandem (EXPAND)
- Tandem to LAN (TCP/IP)
- Tandem to WAN (TCP/IP)
- Tandem to host (TCP/IP)
- Tandem to client connections (TCP/IP, ASYNC, MODEM)

Special security considerations apply to each.

8.1 Tandem to Tandem (EXPAND) Networks

This is a peer-to-peer type of network using a proprietary protocol where each Tandem system is recognized as a separate stand-alone node to all other Tandem systems in the network. This means that each node has both its own stand-alone local security issues separate from the network, as well as those network security issues inherent to the EXPAND network. After user session-level network connections have been established between nodes (remote logon) for distributed processing, the EXPAND connections appear as a seamless connection to the users. This seamless appearance requires the file security already be set up to allow the application/user access to the data files on the remote Tandem node.

The user is not involved in the active network session establishment and can in fact access the data (as a distributed database) through the EXPAND network from a process local to the user's node (as centralized processing). This gives the appearance of one large Tandem system to the user, unless special application considerations need to be addressed to ensure the physical location of the distributed databases between the Tandem nodes.

For a command-level user to be allowed access from one Tandem node to another Tandem node in the EXPAND network, the SA on each relevant Tandem node must set up a REMOTEPASSWORD for that userid on each Tandem node. The appropriate file security to allow successful network processing of the application functions the user is attempting will also be set. Safeguard may be used to aid in the user authorization management of EXPAND network access.

The EXPAND networks can be configured in Star, Ring, or Hybrid topologies. Any two Tandem nodes in an EXPAND network can be connected with a single connection or multiple connections between those two nodes. This is referred to as Single-line EXPAND or Multi-line EXPAND respectively. When Multi-line EXPAND (multiple connections) between any two nodes is established, the Tandem EXPAND network management software of Kernel in each of those two nodes is capable of using all connections simultaneously between that pair of nodes.

This provides an aggregate bandwidth between these nodes of the total bandwidth of all EXPAND connections between the pair of nodes. The EXPAND network management software for all nodes in the EXPAND network are also capable of determining what is the best path to route any packet of traffic (based on an estimated time to route a packet) from its source node to its destination node.

These Tandem nodes can be physically connected together simultaneously via several different types of communications lines. Any pair of Tandem nodes can be connected with their Bit synchronous (Bitsync) or Byte synchronous (Bytesync) ports on each node. These connections can use RS232, RS449, or V.35 (Institute for Electrical and Electronic Engineers [IEEE] standard) interfaces over direct-connect physical cables with modem eliminators, over leased, dial-up, X.25, or frame relay telephone line with modems, or with a Control Service Unit/Data Service Unit (CSU/DSU). Tandem nodes can also be connected using their LAN connections. Issues that must be addressed are user remote access, process remote access, distributed database, remote passwords, and remote userids. All of these must be pre-established by the IAO or the SA.

- *The IAO or their approved representative will set, on each system where EXPAND network access is required, the* ***REMOTEPASSWORDs*** *for the appropriate userids.*

- *The IAO will ensure the appropriate file security to allow successful network processing of the application functions the user is attempting to access has been set.*

- *Network management tools will be secured so only the System Administration group will have access to them.*

CMI	Used to manage communications lines.
COUP	Configuration Utility Program.
CUP	Used to add and remove hardware without a system outage.
NETCOM	This utility is used to configure Distributed Systems Network Management (DSNM) configuration and database files.
SCF	Used to manage communications lines. Intended as a replacement for CMI.

Figure 8-2: Minimum List of Network Tools Table

- *Access to the EXPAND network (remote passwords) will be controlled by the IAOs of the systems involved.*

- *Limited TACL users will not be allowed access across the EXPAND network to another node.*

8.2 Tandem to LAN Network Connections

A Tandem system can connect directly to a LAN in a variety of ways. The Tandem system could connect from one of its LAN controller ports via a direct connect cable to an existing Ethernet segment or a Token Ring LAN, and may support various protocols such as the following:

- TCP/IP (Transmission Control Protocol/Internet Protocol)
- ATM (Asynchronous Transfer Mode)
- FDDI (Fiber Distributed Data Interface)

Users can access the Tandem system via a TCP/IP Telnet, FTP, or IXF protocols from their client PC provided they have the appropriate software and IP stack. Therefore, LAN-related networking security issues are of concern. Refer to the *Network Infrastructure STIG* for these issues. All TCP/IP protocols not specifically authorized in this Tandem STIG will be blocked and prevented from communications with the Tandem systems over the LAN and WAN.

- *The IAO will ensure the appropriate LAN Internet Protocol (IP) addresses, IP filters, masks, Gateway services, and type access permit/deny lists are set and maintained in accordance with the Network Infrastructure STIG.*

8.3 Tandem to WAN Connections

A Tandem system can connect directly from one of its Bitsync or Bytesync ports to a WAN via a router port. Tandem can also be attached to the router via an Ethernet segment or Token Ring LAN port using the TCP/IP protocol. Therefore, WAN-related networking security issues are of concern. For router and WAN-specific security issues, refer to the *Network Infrastructure STIG*.

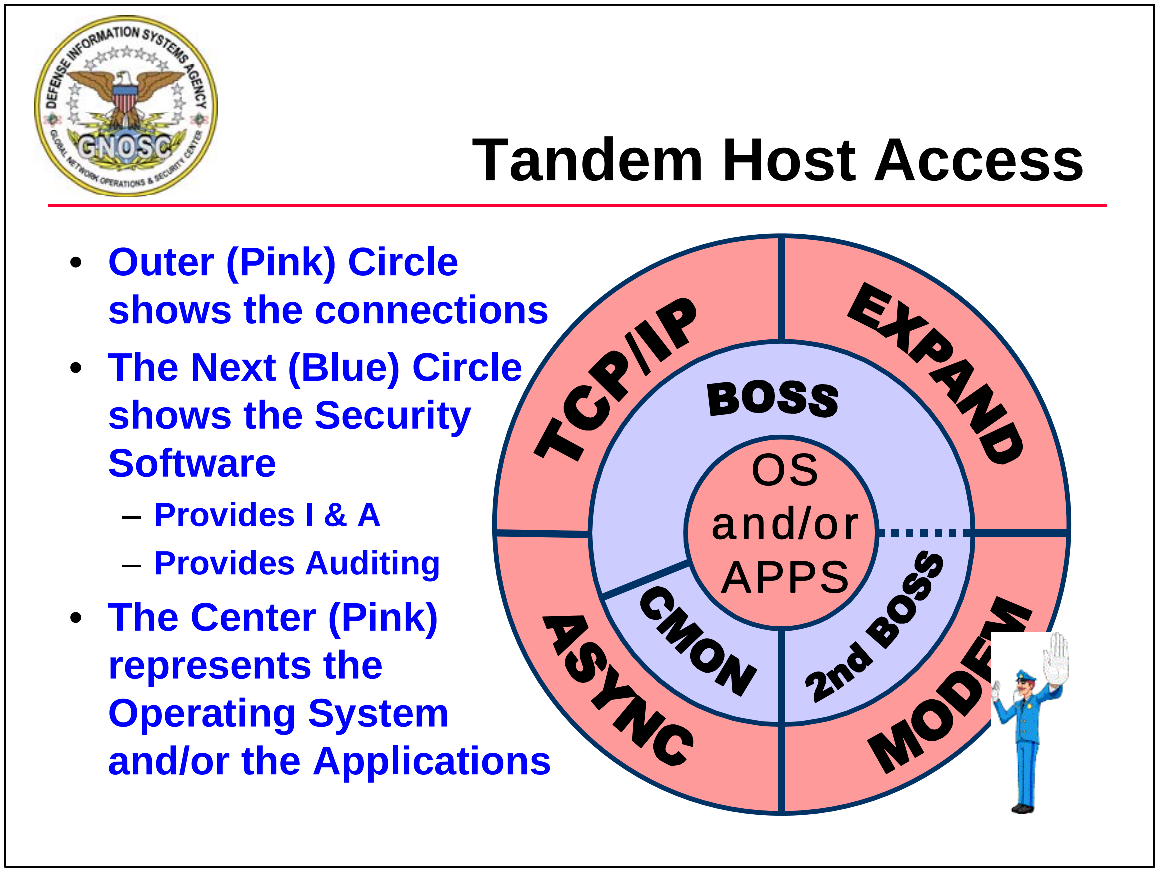
- *The IAO will ensure that the appropriate WAN IP addresses, IP filters, masks, Gateway services, and protocol-type access permit/deny lists are set and maintained in accordance with the Network Infrastructure STIG.*

8.4 Tandem to Host Network Connections

A Tandem system can connect directly from one of its Bitsync or Bytesync ports via a direct connect cable or a leased, dial-up, X.25, or frame relay telephone line using standard RS232, RS449, or V.35 interfaces, with modems, a CSU/DSU, or modem eliminators to a host system. These can be RJE, SNA LU6.2, SNA, or terminal support functions. Therefore, host-related networking security issues are of concern. Refer to the various host-system STIGs, the *Network Infrastructure STIG,* and the *STIG on Enclave Security* for these issues.

- *The IAO will ensure that the appropriate I&A security is performed on the Tandem system, then again prior to the user logging on to the host system in accordance with the appropriate STIG before executing any functions on the Host.*

8.5 Tandem to Client Connection



Tandem Host Access

- Outer (Pink) Circle shows the connections
- The Next (Blue) Circle shows the Security Software
  - Provides I & A
  - Provides Auditing
- The Center (Pink) represents the Operating System and/or the Applications

Figure 8-3: Tandem Host Access

A Tandem system can be connected to a client in any one of several ways. A connection may be from a connected Async, Bitsync, or Bytesync ports (with a direct connect or leased cable). Other connections would include dial-up, X.25, or frame relay telephone line using standard RS232, RS449, or V.35 interfaces, with modems, a CSU/DSU, or modem eliminators to a client (PC or terminal). In addition, client connections are available through LAN/WAN connections (e.g., over a TCP/IP Telnet protocol, attached to either an Ethernet segment or a Token Ring connection).

8.5.1 Inactivity Device (Port Level Lockout)

Inactivity device lockout occurs for users in cases such as excessive error rates that cause user connections to drop. These excessive error rates are based on exceeding threshold levels as described and established in the system configuration.

Systems will be set to terminate or lock out a user session after 15 minutes of inactivity. As an option, the timeout value may be lengthened to 30 minutes by the IAM, if the IAM documents each system extended and explains the basis for this decision. The IAM may set selected userids to have a timeout of up to 60 minutes in order to complete critical reports or transactions without timing out if the following three criteria from the *DISA Computing Services Security Handbook, Version 3, Section 3.13, Remote Access, Item 5. Time Outs, Sub-paragraph c,* can be met:

1. The timeout exception cannot exceed 60 minutes.

2. A letter of justification that fully documents the user requirement must be submitted to and approved by the site IAM. In addition, this letter must identify an alternate means of access control for the terminal(s) involved. Examples include a room that is locked at all times, a room with a cipher lock to limit access, and a password-protected screen saver set to 15 minutes or less.

3. The requirement must be revalidated on an annual basis.

Finally, the timeout may be lengthened beyond the previously mentioned specifications or eliminated for operational reasons with concurrence of the Designated Approval Authority (DAA).

- *The IAO will ensure the error rate parameters are configured on the communications ports. For example, the following parameters must be configured in the Tandem system as appropriate for the communications ports:*

  - *Retry counts threshold*
  - *Retry delay*
  - *Timeout delay*
  - *Number of packets allowed before ACK/NAK is required*

- *Local policy will be established to ensure users do not leave their unsecured Tandem system connections unattended; this could be accomplished by the user logging off the computer or an inactivity lock executed on all systems, to satisfy the following criteria:*

  - *The IAO will set the inactivity timeout lock for selected terminals (PCs) for up to 15 minutes.*

  - *The IAM will set the inactivity timeout lock for selected terminals (PCs) for up to 30 minutes after documentation is established that reflects each system that is extended and the basis for the decision to extend these systems beyond 15 minutes.*

  - *The IAM will set the inactivity timeout lock for selected userids for up to 60 minutes after documentation is established that reflects each extended system, providing an explanation of the basis for this decision, and reflects the IAM approval for the extension.*

  - *Finally, the DAA will approve setting the inactivity timeout lock beyond the previously mentioned specifications or will approve eliminating the timeout lock for operational reasons.*

8.5.2 Data in ASCII Text Form

Data being transmitted and received from the client workstation or terminal is *always* going to be in plain readable ASCII text. This includes the transmission of user logon and password information. If an unauthorized person can access the data being transmitted and received from the client (e.g., with a LAN Analyzer, a sniffer, a data scope, or a Software Trace Facility), the security of the data is *at risk.*

A potential countermeasure is data encryption. This could be at a software level (e.g., a PC terminal emulator with encryption software designed into it and a corresponding software component on the Tandem system). Optionally, hardware encryption devices could be installed at the client's Point of Presence (POP) into the LAN/WAN and the Tandem's POP into the LAN/WAN.

8.6 Inter-network Protection

Unauthorized access must not be allowed from the Internet to the Tandem system. The only LAN/WAN access to the Tandem system that is allowed is from the Trusted Network and will be a Telnet established TCP/IP connection. The user's PC will access the Tandem system with a Tandem support device terminal emulator (e.g., outside view, 6530, or 3270). This access must only provide an application-level (Pathway) access, and only when it has been assured that no command-level access is available through that application. Command-level user access must not be allowed through this LAN/WAN access.

Any FTP access to/from the Tandem system will be from the Trusted Network and requires a special SLA to be signed by the user, and the user needs to send the Tandem system a valid Kernel userid and password as established by the IAO. The only FTP commands that are allowed/supported are GET, PUT, MGET, and MPUT. Only after the user has passed a tightly controlled access is the user allowed to use these commands.

NOTE: It is implicit in policies and guidance that all communication sessions' support encrypted links. FTP does not support encrypted sessions. If FTP is being used, now is the time to start migration to a communications protocol, which supports encrypted links.

Any Simple Mail Transfer Protocol (SMTP) access to/from the Tandem system will be from the Trusted Network. The TCP/IP port that supports SMTP must be disabled unless there is a specific operational requirement for the SMTP traffic to the Tandem site.

- *The IAO will coordinate with the NSO to ensure **non-secured access** is not allowed through the Internet to the Tandem system.*

- *Access (Telnet, FTP) will not be permitted to the Tandem system through the LAN, other than application user-level access on a Trusted Network or users using an encrypted connection.*

- *More than the approved FTP commands (i.e. **GET**, **PUT**, **MGET**, and **MPUT**) will not be available to any application-user-level access.*

- *SMTP access will only be allowed if a specific operational requirement exists for this service, and is approved in writing. Otherwise, this service, along with the associated TCP/IP well-known port numbers, will be disabled.*

When setting up the system, SMTP access is by default allowed even if a specific operational requirement does not exist for this service. In addition, the SMTP associated TCP/IP well known port numbers are enabled. Because the default state is active/enabled/allowed, the IAO and SA need to ensure that this service and the associated ports are configured according to their operational requirement.

- *Additional I&A will be required to be performed for all users accessing the Tandem system through the Internet unless a pre-approved Field Security Operations enhanced I&A mechanism is being used.*

- *There will be no access to the Tandem, to include access from the Internet without the knowledge of the IAO and the SA.*

- *There will be no access to the Tandem without session auditing.*

- *The IAO will ensure all TCP/IP well-known port number services not specifically required will be disabled.*

- *The IAO or SA will ensure documentation is maintained to reflect the TCP/IP port number services authorized and enabled on the Tandem system.*

- *The utilities and commands will be used to modify the appropriate files by using the default filenames to ensure the Tandem TCP/IP functions, protocols, services, and ports are appropriately configured and secured, as described in the following table.*

COMMAND	***DEFAULT TANDEM FILE NAME***	***DESCRIPTION OF EFFORT***
EDIT	$SYSTEM.ZTCPIP.PORTCONF	Remove entries for unauthorized ports.
FUP SECURE and FUP GIVE	$SYSTEM.ZTCPIP.PORTCONF	Prevent unauthorized reconfiguration and access.
EDIT	$SYSTEM.ZTCPIP.SERVICES	Remove unauthorized services entries.
FUP SECURE and FUP GIVE	$SYSTEM.ZTCPIP.SERVICES	Prevent unauthorized reconfiguration and access.
EDIT	$SYSTEM.ZTCPIP.PROTOCOL	Remove entries for unauthorized protocols.
FUP SECURE and FUP GIVE	$SYSTEM.ZTCPIP.PROTOCOL	Prevent unauthorized reconfiguration and access.
EDIT	$SYSTEM.ZTCPIP.SMTPCONF	Remove entries for unauthorized SMTP gateways.
FUP SECURE and FUP GIVE	$SYSTEM.ZTCPIP.SMTPCONF	Prevent unauthorized reconfiguration and access.
FUP SECURE and FUP GIVE	$SYSTEM.ZTCPIP.NAMED	Prevent unauthorized Domain Name Service (DNS) reconfiguration and access.
EDIT	$SYSTEM.ZTCPIP.RESCONF	Remove entries for unauthorized DNS.
FUP SECURE and FUP GIVE	$SYSTEM.ZTCPIP.RESCONF	Prevent unauthorized reconfiguration and access.
EDIT	$SYSTEM.ZTCPIP.HOSTS	Remove entries for unauthorized host names.
FUP SECURE and FUP GIVE	$SYSTEM.ZTCPIP.HOSTS	Prevent unauthorized reconfiguration and access.

- *The IAO and the SA will ensure that TCP/IP functions or port numbers, TCP/IP services, protocols, SMTP Gateway service, Domain Name Resolver, DNS service, and default host names are configured and secured properly to prevent unauthorized access and/or reconfiguration.*

- *The IAO will ensure that all unauthorized TCP/IP service program files are secured to allow SUPER.SUPER access only.*

To ensure a specific access path from a trusted LAN/WAN TCP/IP network to the Tandem systems, only the use of static IP addresses, static IP address masks, static gateways and static windows will be allowed. All users are required to submit the appropriate userid and password to gain access to the Tandem sites. All Tandem system LAN TCP/IP connections must have static IP addresses. Note that without the IS to IS Inter-domain Routing Protocol (IRDP) listed in the Protocol file, the use of static default routes is required by TCP/IP. After TCP/IP has been appropriately configured, use FUP to secure it from unauthorized access and modification. For implementation details, see *Appendix C, Initial Tandem System Setup*.

- *The IAO and the SA with the NSO will establish all Tandem systems LAN TCP/IP connections with static IP addresses, static address mask, static gateways, and static windows.*

- *The IAO or the SA will ensure that the access to the Tandem is in accordance to the "Packet Filtering Policy" and "TCP/UDP Port and Service Filtering Guide" of the current Network Infrastructure STIG and the STIG on Enclave Security.*

- *The IAO or the SA will ensure that filters will be in place to manage all network traffic not filtered by the routers or firewalls.*

8.6.1 Kerberos (Network Authentication Protocol)

Kerberos is a Network Authentication Protocol that enables strong authentication for both clients and server applications. This product is available free from the Massachusetts Institute of Technology (MIT) as well as being available in many commercial products.

With computer systems being connected to LANs and various types of networks, there is a need to secure data on the system and the data that is being transmitted on the network connection, so that unauthorized users do not have access to that data.

The more extensive the encryption, the more resources the process will take. Because of the system resources, the Kerberos protocol can be customized to work with different security needs.

NOTE: For more information, refer to the Compaq/Tandem Total Information Manager (TIM) documentation PC program.

8.7 Communications Servers

The Tandem systems can function as a communications front-end processor to mainframe hosts, or as a communications front-end server to a LANWAN network (such as a gateway into the LAN/WAN network). Refer to the *Network Infrastructure STIG* for special considerations and more details for setting up Gateway communications servers on LANs. A future release of this STIG is scheduled to address more Tandem-related issues for communications server gateways into LAN/WAN networks.

When Tandem systems are used as front-end processors supporting user terminal access to an

IBM host system, the Tandem application software requires the user to pass a standard I&A logon by entering a valid userid and password.

- *All pass-through users will be required to go through BOSS I&A prior to being allowed access to the back-end host system.*

- *Pass-through only users (i.e., users who do not do any Tandem processing except to use the Tandem system as a front-end to pass-through to a host) will not be granted further access to the Tandem system.*

8.8 Tandem Network Management

Tandem sites can function as open system servers to a multiple and varying user client base. These clients could be dumb terminals (3270, 6530, etc.), Personal Computers, other servers, or devices attached to another host system that is networked to the Tandem system. The following sections address some security issues as related to TCP/IP LAN/WAN attached clients accessing the Tandem system.

8.8.1 Tandem (Open Systems) Network Management Issues

Tandem does have the ability, by the use of EMS filters and EMS distributors (EMSDIST), to send warning and error messages (in the Simple Network Management Protocol [SNMP] form) to another device. These other devices could be executing a process, such as Hewlett Packard's OPENVIEW monitor (MIB format is required), and display a graphic representation of the network status. Conversely, Tandem can receive warning and error SNMP messages from another device through the EMS collectors, and forward them through an EMS filter to a Network Management Station or display system/software/device (such as a PC running the COTS TIC [Telecommunications Interface Converter] product).

8.8.2 Screening and Filtering Requirements

Packet filtering can be set on the Tandem LAN port and must be considered if it is used for TCP/IP services (e.g., FTP, DNS, Telnet, etc.). Many SAs may consider that it would be more efficient to handle the filtering on a firewall or a router where the cost of the overhead cycles would be cheaper than on the Tandem. However, defense-in-depth promotes layering of security at each level of a network.

The defense-in-depth strategy is a layered approach to security that leverages technology, people, and procedures to greatly enhance the security of DOD assets. Initially, this strategy was developed to address the evolving threats and the vulnerabilities posed by attack scenarios. However, at the same time, the strategy has, and must continue, to evolve to respond to changing technologies. With respect to DOD networks and network information systems, this objective is realized through a layered approached by applying multiple layers of security using different mechanisms and security products. Any one layer does not provide an adequate protection, but taken as a whole, the layers protect DOD information systems and networks against attacks. In addition to the SA setting packet-filtering rules for the Tandem (refer to the *Network*

Infrastructure STIG and the *STIG on Enclave Security* for a list of items to be filtered), the SA must work with the NSO to ensure the additional layers of protection are achieved to protect the Tandem.

- *The IAO will coordinate with the NSO and establish procedures to ensure that all LAN traffic to and from the Tandem systems is legitimate and authorized.*

- *The IAO will ensure that unauthorized traffic is not routed, broadcast, or bridged to a Network.*

8.8.3 Simple Network Management Protocol (SNMP)

8.8.3.1 SNMP Overview

The Simple Network Management Protocol (SNMP) is a widely deployed protocol that is commonly used to monitor and manage network devices. Although SNMP is the most used protocol for network management, it is not a very secure protocol. As with any network-connected host, it is recommended not to expose unprotected hosts running SNMP outside of your local area network (LAN) or enclave. Firewalls protecting your LANs/Enclaves should be checked to make sure that they are configured to block the ports that SNMP uses (port 161 and 162). In the event SNMP is required outside of the LAN/Enclave, it should be limited be specific IP addresses of those hosts authorized this access. The SNMP community strings provide a method to identify systems that are authorized to talk with each other over SNMP. Anyone using SNMP should change the default community strings from "public" for SNMP get operations and "private" (for SNMP set operations). Each of these community strings should be set to unique values, protected the same as passwords and changed at least every 90 days.

Vulnerabilities in SNMP request and trap handling could possibly cause denial-of-service, service interruptions, and unauthorized access. It is possible vulnerabilities are exploitable without knowing a valid SNMP community name and without knowing the actual IP address of the subject. Refer to IAVM or DOD-CERT for current information on SNMP vulnerabilities.

- *The IAO will ensure that each host is protected by configuring border network devices to block the SNMP service ports of 161 and 162.*

- *In the event SNMP is required outside of the LAN/Enclave, the IAO will maintain a list of hosts and the specific IP addresses of those hosts authorized this access.*

- *In the event SNMP is required outside of the LAN/Enclave, the IAO will ensure each host is protected by configuring border network devices to only permit the specific IP addresses of those hosts authorized this access.*

- *The IAO will ensure the default community string names for SNMP get operations and SNMP set operations have each been changed to a unique value and are protected as passwords, even if SNMP is not being run on the host.*

8.8.3.2 SNMP Management Information Base (MIB)

SNMP uses MIBs (Management Information Bases), as defined in RFC 1213, to manage different parts of a network. Each part of the network would require a MIB. Individuals can create MIBs for use in managing the network as long as they conform to the RFC 1902 Standard.

- *The IAO, in conjunction with the SA, will ensure that all MIB files, used by SNMP, will be secured so only the System Administration user has access to them.*

NOTE: The MIB files need to be owned by Super.Super and will have the security of “OOOO”.

There is a utility on Tandem called MIBCOMP. This utility is used to compile/parse MIB. When you are using MIBCOMP, you will have an output file. An output file will be named starting with RFC and are code 101 files.

For additional information on the MIBCOMP Utility, see ***Using the MIB Compiler***, Chapter 3 of the *SNMP Manager Programmer’s Guide*, found in the Total Information Manager (TIM) documentation PC program.

- *The IAO, in conjunction with the SA, will ensure the MIBCOMP utility is secured so that only the System Administration user has access to it.*

NOTE: The MIBCOMP Utility needs to be owned by Super.Super and the security of “OOOO”.

8.8.3.3 SNMP IAVMs

IAVMs have been issued concerning the subject of SNMP. Always check with IAVM or DOD-CERT for current information on existing or new SNMP vulnerabilities. 2002-A-SNMP-003-01 and 2002-T-SNMP-003-01 are the currently applicable IAVMs.

2002-A-SNMP-003-01.

This alert does not show up on the IAVM VS08 report, as of the date of this STIG, but is applicable, if you are running SNMP. This is in the process of being corrected, as this IAVM should be on the VS08 report.

NOTE: This item will be checked for compliance during SRRs.

These potential SNMP vulnerabilities are applicable to SNMPv1 trap handling and SNMPv1 Request handling. Compaq's findings (to date) regarding the SNMPv1 issues on the NonStop Himalaya Servers are printed word-for-word from their Security Advisory: SRRT0779, and are as follows:

Compaq NonStop Himalaya Servers:

The Compaq Himalaya NonStop Kernel prohibits execution of code on the stack or heap by hardware TLB permissions (read/write only), preventing Trojan horse attacks by embedding code within the buffer overflow area. However, process ABENDs can occur.

The SNMP agent ABENDs in the c06-snmpv1 buffer-overflow tests. This affects forwarding trap messages and/or sending info responses to SNMP managers.

Sub-agents use IPCs to communicate with the SNMP agent, so they cannot be directly attacked. More importantly, sub-agents are confined to information only requests, so they cannot be used to configure/manage their sub-systems. Investigation and analysis is continuing and further updates will be provided.

Resolution:

IPMs to address the ABEND problem of the SNMP are in development and will be released as soon as verification is complete. Availability of these IPMs will be announced in future updates. The exposure to SNMP agent ABENDs can be reduced by running the SNMP agent as a process-pair or by configuring auto-restart in the Persistence Manager.

2002-T-SNMP-003-01.

This technical advisory will show up on the IAVM VS08 report, but this particular one is not applicable to the Tandem and will have to be reported as such when updating the IAVM vulnerability information.

9. TANDEM SYSTEM BACKUPS

On Tandem systems, file and database backup and recovery issues are addressed with two separate functions:

- File-level backup/restore of all data
- Transaction-level on-line/recover files of audited data only

NOTE: This should not be confused with the Disk Dumps that are already documented in the Tandem Attack/Recovery procedures (see *Section 7, Recovery from a System Compromise/Alteration*).

The use of backups is an integral part of system security. If an operating system or a file is maliciously or inadvertently deleted or corrupted, the system backup provides a valid replacement for the damaged item. In addition to being a vital part of system security, system backups are required for disaster recovery programs.

9.1 File-level Issues for Database Backup and Recovery

The two types of system backups to be used are full and incremental (partial) backups. The full system backups will be done periodically to create a baseline that can be used for recovery. Baseline backups should be done before and after major upgrades and/or changes to the system.

Included with this baseline backup will be sufficient documentation in the site SOP that allows the IAO to verify the system health following a potential or verified system attack. (Refer to *Section 5.2, System Integrity (Operating System Software)*, for more information regarding use of the baseline.) These baseline sets of full system backups will be created as determined by the IAO or at least bi-annually and maintained for at least one year.

- *The IAO and the SA will develop local policy and implement Standard Operating Procedures (SOP), for COOP/DRP purposes, for system backup and restoration of the complete system to include the following at a minimum.*

  - *The two types of system backups to be used are full and incremental.*

  - *A schedule for full and incremental backups.*

  - *Detailed backup procedures.*

  - *Detailed restore procedures.*

  - *Customer requirements include a copy of the Memorandum of Agreement (MOA) and a copy of the SLA.*

  - *Storage and retention procedures for backup media.*

  - *System backups will be retained for one year.*

  - *Procedures to keep backup media in a controlled access environment with one copy kept in an off-site controlled access environment.*

  - *Schedule and methodology for testing restoration procedures.*

- *The IAO will ensure procedures are in place to secure backup tapes stored at a remote location.*

NOTE: A remote location for backup tapes is a location that is far enough away from the original location that if there is a disaster and the site is damaged or made inoperable, the backup tapes can be taken to an alternate location and restored on a system at the alternate location in order to restore operations.

9.2 Transaction-level Audited Database Backup and Recovery

The Tandem systems also provide the ability to maintain the entire database in a consistent state by use of data transaction audit trails and periodic on-line dumps of audited files to recover data in the audited files to a transaction level. These features provide the ability to recover all files in the database to a single transaction level of consistency.

The audit trail logfiles need to be rolled to tape periodically (this is referred to as performing an audit trail dump). TM/MP requires that an on-line dump of all audited data files will be done periodically to create a set of backup tapes to function as a baseline that can be used for database recovery if required. When a new on-line dump is performed, TM/MP automatically retains the previous on-line dump and any audit trail dump information. It is recommended that on-line dumps be performed at least following major upgrades, major changes to the database, and/or changes to the system configuration.

When the audited database is in an initial consistent state, and the applications are quiescent, the TM/MP INITIALIZE TMF command will be executed. The execution of this command instructs TM/MP software to establish a starting point for auditing the entire database. TM/MP will automatically scratch the tapes associated with all previous on-line dumps and audit trail dumps following the execution of the INITIALIZE TMF command. Therefore, following the execution of the INITIALIZE TMF command, the IAO will ensure that a new TM/MP baseline backup on-line dump is performed.

- *The IAO and the SA will develop local policy and implement SOPs for system backup and restoration of the audited data through TM/MP, the system transaction audit trail dumps, on-line dumps, and recovery functions only to include the following at a minimum:*

  - *Customer requirements include a copy of the MOA and the SLA.*

  - *Storage and retention procedures for on-line dump and audit trail dump backup media*

- *Procedures to keep on-line dump and audit trail dump tape media in a controlled access environment, with one copy kept in an off-site controlled access environment*

- *Schedule and methodology for testing transaction recovery procedures to include verification of database update transaction backout*

- *A schedule for audit trail dump and on-line dump backups*

- *Detailed on-line dump and audit trail dump procedures*

- *Detailed roll forward recovery and backout procedures*

- *Procedures for maintaining a historical file of the TM/MP configuration control files of the system*

9.3 RDF Transaction-level Remote System Database Recovery

The Remote Database Facility (RDF) provides a transaction-level mirroring of data to an alternate backup node (site). This product requires TM/MP on each node, an EXPAND link between the systems, sufficient data storage on the backup node to hold the entire database being backed up from the production node, and the operating system releases on each system to be in synchronization.

- *Prior to the use of the Remote Database Facility (RDF), the IAO will coordinate efforts with Field Security Operations to address all related security concerns, which will include the (receive) system for the RDF database to also be STIG compliant.*

This page is intentionally left blank.

10. GENERAL FACILITY MANAGEMENT CONCERNS

The following sections set guidance that applies to all Tandem Automated Information Systems facilities and that will be accomplished in accordance with the *Computing Services Security Handbook*. Each area of concern is addressed in a separate section.

10.1 Facility and Location Security

The intent of this document is not to define the facility security guidelines, but to only address the security requirements of the Tandem physical system to be maintained in a secured access area.

- *The environmental conditions (air conditioning, power requirements, etc.) will be, in accordance with standard Tandem guidelines, dry (acceptable humidity range) and moderately cool (acceptable temperature range), and the environmental controls will be secured to prevent accidental or intentional changing of the settings.*

  (Refer to the operating system environmental requirements as documented in Tandem's Total Information Manager (TIM) manual series on CD-ROM for more details.)

The Uninterruptible Power Source (UPS) product must deliver not just reliable backup power in the event of a blackout, but clean, steady power around the clock to prevent data loss and equipment failure. The UPS must be either on-line or line-interactive UPS products. Most on-line UPSs provide dual-source power to continuously condition and correct the incoming power. They take Alternating Current (AC) from the outlet, convert it to Direct Current (DC), regulate it, and then convert it back to AC power.

- *The IAO or the SA will ensure that each Tandem system is on a UPS.*

- *All systems will be located in a controlled access (e.g., restricted) area.*

NOTE: These areas will be physically controlled using approved locking mechanisms.

- *When a system is installed in an open area, such as an office environment (not the computer floor), an individual physically located within close proximity to the system will be charged with visual accountability and immediate notification to the IAO or NSO of any suspicious, system related, activity.*

- *Only the IAO, SA, NSO, or a designated control officer will authorize entry to the controlled access area.*

10.2 DISA Security Handbooks

The sites will adhere to guidelines set forth in the *Computing Services Security Handbook* pertaining to the physical control and location of IS assets. For further information, also reference *IAO Responsibilities for The National Computer Security Center's AIS (Light Blue Book NCSC-TG-027 Version-1), Section 3.6, Physical Security Requirements*.

10.3 Distributed Processing and Client System Protection

There may be occasions where a user will need to process information at a different location than where the information originated. These locations are considered as Off-site. Off site is also considered as processing data at a different location than where the data was originally stored. Some of the ways would be to put the data on a portable media, such as floppy disk, backup tape, CD-R and Laptop. Others are such as accessing a system remotely and downloading information to your local machine. When processing data in any of the above manners, it is the responsibility of the person that removed the data from the original system to ensure that the proper handling of that data.

Only GFE equipment is approved for off-site use for processing Government Data. Home computers, laptops, remote dial-up terminals, and notebooks used off-site by an increasing number of employees are often not secured. The off-site storage of data on backup tapes or disk volumes needs protection. Refer to *DISA Computing Services Security Handbook*, *Section 3.14 and Remote Access STIG,* for additional guidance.

- *The IAO will ensure procedures are in place for managing all off-premise processing.*

10.4 System Maintenance and Repair Issues

Tandem engineers or subcontractors perform all hardware repairs to maintain certification and current firmware revisions. The IAO will establish procedures so that when repairs are being performed, an authorized, trained Government representative is monitoring and auditing the functions performed on the Tandem system in accordance with the *DISA Computing Services Security Handbook, Section 3.21*.

- *Authorized individuals (e.g., Tandem engineers or site employees) will be the only personnel performing system repairs.*

- *The passwords for all userids used by uncleared Maintenance personnel will be changed after the maintenance is completed and the passwords will be secured at the site, and an entry made in the site SOP that it has been accomplished.*

- *The IAM/IAO will create and enforce procedures for ensuring that all system repairs are in accordance with the local CCB.*

10.5 Client Terminal (PC/Workstation) Concerns

The intent of this document is not to define the security guidelines for PC/workstations except for special considerations of access security requirements of the Tandem physical system to be maintained in a secured access area. Refer to the *DISA Computing Services Security Handbook, Section 3.14*, the *NSA NT Guide*, and the *DISA NT Addendum* for guidelines on PC workstations. Tandem systems support many client-type devices. All the supported devices will maintain security of data and user passwords.

10.6 Standard Password Protection

Standard user password protection is a concern for all systems and Tandem NSK users are no exception. Passwords will be established and maintained in accordance with the *DISA Computing Services Security Handbook, Section 3.13*.

- *The IAO and the SA will ensure that all users follow the password standards.*

- *All devices, where possible, will be password protected.*

- *All default system passwords will be changed immediately when the system is first installed and configured and prior to allowing any user access.*

- *All known backdoor userids and associated passwords will be removed.*

- *Passwords will be created using accepted generation schemes (e.g., Computing Services Security Handbook or password generators).*

- *The IAO will record all system level passwords, and what they grant access to, place them in a sealed envelope and place the sealed envelope in a safe accessible by key Operations personnel for use during emergencies.*

10.7 Dial-up Access and External Phone Line Connections

Modems can provide an unchecked gateway to sensitive data within the DOD's computing boundaries; therefore, there is a need to secure the modems and the equipment (Host) to which they are connected. Remote dial-up access security has become an issue of great concern in DOD. An installation security policy should not only examine network protection from any Internet access, but also against authorized dial-up access. The remote access infrastructure should determine that a dial-up user is indeed who they say they are, restrict access to authorized network resources and services, and log the entire event. These procedures will provide authentication, authorization, and auditing.

Special considerations of external phone line connections and modems as related to the Tandem system are addressed in this section. This document does not address all security issues related to external phone lines and related equipment, but only the relationship to the Tandem system. Additional information can be found in this STIG, in *Section 4.2.2.3, Dial-up Security*. Refer to the *Network Infrastructure STIG,* the *STIG on Enclave Security*, and the *DISA Computing Services Security Handbook* for more detailed information on this subject.

For sites that have remote access to the Tandem system via a local Remote Access Server (RAS), all users that have access to the Tandem will first connect into those RAS servers and then use Telnet to access the Tandem, as if they were in the office. This will give multiple levels of Security. For the instance where this is not possible, the IAO will document the reason for such direct access.

- *When dial-up ports exist on the Tandem system, the IAO will maintain a list of all personnel authorized to access (dial into) the dial-up ports.*

- *When dial-up ports exist on the Tandem system, the processes for those dial-up ports will not have full command-level access, but will be limited to perform only the specific need. Any exceptions will be documented by the IAO.*

NOTE: The IAO will need to document the following information for users that require this type of full command-level access:

- User’s name
- User’s phone number
- Userid
- User’s node name
- Date range (period access is needed)
- Detailed justification for requiring the access

- *When dial-up ports exist on the Tandem system, the processes executing on the Tandem system supporting user access on all dial-up connections will be very closely monitored and tightly controlled in accordance with Section 4.3.2, Audit Trails.*

- *When dial-up ports exist on the Tandem, the IAO will ensure the dial-up modems are configured to use enhanced identification and authentication or the modems will be disabled.*

Lack of enhanced identification and authentication can make it easier for a hacker to gain access to a system causing loss or compromise of data or denial of service.

***NOTE**:* All modems must include adequate safeguards such as:

- Enhanced identification and authentication mechanisms
  - Dial-Back systems
  - Public Key Infrastructure (PKI) Certificate
  - Smart Card or random password generators
  - Caller ID or Security Access Control System (SACS)
- Automatic log out upon call termination
- Automatic hang up upon caller log out
- Remote configurations disabled
- Physical protection from unauthorized access
- Configure modems for either outgoing or incoming calls - not both
- Call forwarding disabled Third party billing disabled

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

Government Publications

Department of Defense CSC-STD-002-85, "DOD Password Management Guideline," 12 April 1985.

Department of Defense CM-400-260-01, “Software Requirements Specification (SRS) for the Network Management (NM) Functional Area of the Defense Information Infrastructure (DII),” 8 July 1997.

DOD Directive 3020.26, "Continuity of Operations (COOP) Policy and Planning," 26 May 1995.

DOD Directive 3020.36, "Assignment of National Security Emergency Preparedness (NSEP) Responsibilities to DOD Components," 2 November 1988.

DOD Instruction 3020.39, "Integrated Continuity Planning for Defense Intelligence," 3 August 2001.

DOD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD [C3I])," 12 February 1992.

Department of Defense Directive Number 8500.1,” Information Assurance (IA) 24 October 2002 (ASD [C3I]).

Department of Defense (DOD) Directive 8500.1, "Security Requirements for Automated Information Systems (AISs)," 21 March 1988.

DOD Directive Number O-8530.1, Computer Network Defense (CND), 8 January 2001.

DOD 8910.1-M, "DOD Procedures for Management of Information Requirements," 30 June 1998.

Defense Information Systems Agency Instruction (DISAI) 630-230-19, "Security Requirements for Automated Information Systems (AIS)," August 1991, and Supplement 1, 27 April 1994, and Supplement 2, 27 April 1994.

National Security Agency (NSA), "Information Systems Security Products and Services Catalog" (Current Edition).

Field Security Operations Publications

DISA Computing Services Security Handbook, Version 3, dated 1 December 2000

Tandem Security Checklist

Tandem Security Scripts

Network Infrastructure STIG

Secure Remote Computing Addendum to the Network Infrastructure STIG

NIPRNet STIG

STIG on Enclave Security

UNIX STIG

Web Services STIG

Commercial and Other Publications

Tandem

Tandem's Total Information Manager (TIM) manual series on CD-ROM (includes the following documents and many more):

Operating System Release SOFTDOCs

Guardian 90 Operating System User's Guide

NonStop System Support Guide

NonStop System Operations Guide

Guide to Common Operations Tasks

Tandem Maintenance and Diagnostic System (TMDS) Reference Manual

NonStop Net/Master Rule Management Services (RMS) Management and Operations Guide

Trusted Facilities Manual by Tandem (Part Number 057770, Release S01.00, April 1993)

BOSS

Block Mode Operating Systems Services (BOSS) Quick Start Manual Version 5.0

Block Mode Operating Systems Services (BOSS) User's Guide Version 4.0K

BOSS (Block-mode Operating System Services) User's Guide, Version 4.0, by Cross-El Software Solutions.

Information Systems Security products and Services Catalog Section, Serial No. CSC-EPL-93/001 (pages 4-59 through 4-61).

Audit, Control, and Security of the Tandem NonStop Systems by Ernst and Young (1994).

References (World-Wide Web)

CERT Alerts (from 1988) - **http://www.cert.org/nav/alerts.html**

CERT Coordination Center - **http://www.cert.org**

Compaq Services Software Patches - **http://ftp.support.compaq.com/patches/.new/security.shtml**

Compaq Support Home Page - **http://wwss1pro.compaq.com/support/home/index.asp**

DOD-CERT Home Page - **http://www.cert.mil**

FSO Guides: **http://guides.ritchie.disa.mil/**

Network

Network Information Center (NIC) - **http://www.internic.net/**

NIPRNet Connection Approval Process - **http://cap.nipr.mil**

Tandem

Attla Security Products - **http://atalla.nonstop.compaq.com/**

Security best practices for NonStop Servers – **http://nonstop.compaq.com/view.asp?IO=SECBESTAR**

Tandem Glossary - **http://nonstop.compaq.com/TechPubs/IUG/dtog/GLOSS.htm**

Tandem NonStop Computing - **http://nonstop.compaq.com/**

Tandem Safeguard Security - **http://nonstop.compaq.com/view.asp?PAGE=Safeguard**

Tandem Security Products - **http://nonstop.compaq.com/view.asp?PAGE=Security**

Tandem Technical Reports - **http://www.hpl.hp.com/techreports/tandem/**

APPENDIX B. INTERNET GENERIC PORTS AND SERVICES

The only TCP/IP services that can be made available directly from the Tandem systems are Telnet, (some) FTP, SNMP, and SMTP. Access to these services will be tightly secured and carefully controlled to ensure only secured access from authorized users is allowed. The TCP/IP traffic that is allowed will access the Tandem system through the Trusted Network. The Trusted Network will verify that unauthorized traffic will not reach the Tandem system. In the future, if any additional services from the Tandem systems are deemed prudent, the traffic related to these services will also pass through similar filtering and authorization mechanisms. For a guide to the suggested minimum filtering rules for perimeter routers and firewalls, refer to the *Network Infrastructure STIG*.

Currently only authorized documented TCP/IP services will be available directly from the Tandem systems. All others will be blocked. The way to prevent unauthorized TCP/IP services from being available for users is to secure them using the file system security. This way the only valid Kernel userid that can be allowed to execute these processes is SUPER.SUPER.

```
TACL1>LOGON SUPER.SUPER
TACL2>FUP
>VOLUME $SYSTEM.SYS00
>GIVE (FTP, TELNET), 255,255
>SECURE (FTP, TELNET), "OOOO"
>EXIT
TACL3>LOGOFF
```

To ensure Tandem TCP/IP functions, protocols, services, and ports are appropriately configured and secured as discussed in *Section 8.6, Inter-network Protection*, use the following utilities and commands:

```
TACL1>LOGON SUPER.SUPER
TACL2>VOLUME $SYSTEM.ZTCPIP
TACL3>EDIT PORTCONF
(Delete entries for unauthorized ports)
*GET SERVICES
(Delete entries for unauthorized services)
*GET PROTOCOL
(Delete entries for unauthorized protocols)
*GET SMTPCONF
(Delete entries for unauthorized SMTP gateways)
*GET HOSTS
(Delete entries for unauthorized hosts names)
*GET RESCONF
(Delete entries for unauthorized Domain Name Resolver)
*EXIT
```

```
TACL4>FUP
>GIVE (PORTCONF, SERVICES, PROTOCOL, SMTPCONF), 255,255
>GIVE (NAMED, HOSTS, RESCONF, DNS), 255,255
>SECURE PORTCONF, ”GOOO”
>SECURE SERVICES, ”AOAO”
>SECURE PROTOCOL, “GOGO”
>SECURE SMTPCONF, "OOOO"
>SECURE NAMED, “OOOO”
>SECURE HOSTS, “GOOO”
>SECURE RESCONF, “GOOO”
>SECURE DNS, "OOOO">EXIT
TACL5>LOGOFF
```

APPENDIX C. INITIAL TANDEM SYSTEM SETUP

This is an initial system setup guide to assist in the installation of new systems and will be considered as a recommended guideline. The recommended conventions or examples in this section are not to be considered mandatory. However, they could be helpful in cleaning up security issues and addressing potential problems in existing systems.

Establish system hardware and software configuration.

- Determine what hardware configuration is required.
- Determine what Kernel software is required.
- Establish a $SYSTEM volume and a volume for the Install-related files.
- Determine which terminals in the secured access area must have full command-level TACL access, and of those terminals, which must have a TACL process started on them in the normal system initialization procedure (CIIN file).
- Establish (create) a normal system initialization procedure (CIIN file) including the following functions:

NOTE: The first line should be to reload all CPUs.

```
RELOAD *, PRIME
```

The following commands should also be inserted into the current CIIN file if not already present:

```
ZSERVER /NAME $ZSVR, NOWAIT, CPU x/y
TAPECOM CLEAR NLCHECK
SAFECOM START SAFEGUARD
```

***NOTE*:** x & y is the Primary and Backup CPU that ZSERVER uses.

Next, add default TACL processes discussed above (for secure terminals and the OSP/RMI) and start them in different CPUs.

- Establish the Spooler. (Configure it, create obey files, and cold start it.)
- Establish the volume location (not $SYSTEM) for Install, DSVs, ISVs, and Installs database.

- Create operating system image with the current configuration including the following parameters in the system configuration (CONFTEXT file).

NOTE: The parameter, **SYSTEM_TERMINAL**, is used after system cold load to determine where an initial TACL is to be started. The name of this terminal is configured through SYSGEN and it is started in a logged on state to the SUPER.SUPER userid. This terminal will be one of the two TACL terminals in the secured area that are not controlled by BOSS. In the **ALLPROCESSORS** paragraph, add these parameters if missing from the CONFTEXT file and set to these values.

```
SYSTEM_VOLUME_SUBVOL                $SYSTEM.SYSnn;
BUILD_Z0_PROCESS;
SYSTEM_NAME                         \<name>;
SYSTEM^NUMBER                       <number>;
MAXIMUM_SYSTEMS                     <NODES_per_network>;
TAPE_LABEL_PROCESSING               ENABLED;
INITIAL_COMINT_INFILE               $SYSTEM.CONFIG.CIIN;
SYSTEM_TERMINAL                     $<term>;
STANDARD_MICROCODE                  TANDEM^STANDARD^MICROCODE;
SYSTEM_LIBRARY_CODE_FILES           TANDEM^LIBRARY^CODE^FILES;
SYSTEM_PROCESS_LIBRARY_FILES        TANDEM^PROCESS^LIBRARY^FILES;
SYSTEM_PROCESS_CODE_FILES           TANDEM^PROCESS^CODE^FILES;
FORMATTER_TEMPLATE_FILES            FORMATTER^TEMPLATE^FILES;
FILES_TO_COPY_TO_NEW_SYSTEM         TANDEM^FILES^TO^COPY;
```

- Initialize the current OS image and test to verify that all devices and operating system software functions as anticipated.

- Give ownership of operating system-related files to the SA userid.

- Alter the file system security of the operating system and related supporting files to the appropriate access level.

- Alter security of operating system installation files (DSV, ISV, and database) to the appropriate access level.

- Build general system startup obey files, e.g.,

```
MEASCOM START MEASSUBSYS
TMFCOM START TMF
OBEY SPOOLER.WARMSTRT
```

Next add TACL processes started in different CPUs.
Start BOSS (but not the BOSS terminals).
Start TCP/IP and LAN-related processes.
Define windows, services, TCP/IP addresses, and masking.
Start the applications (i.e., Pathway system and related resources). Then start the BOSS terminals.

Establish super-group users.

- Build TACLLOCL default Enscribe wide for all TACL users.
- Build TACLCSTM files for users.
- Establish a TACLSEGF file (system wide) for all TACL users.
- Set defaults (security, volume, and subvolume) for all existing userids.

Establish conventions and procedures.

- Device Name Conventions, e.g.,

  Tape drives: $TAPE1, $TAPE2, $TAPE3
  Async (Clip4) type Terminals: $A1.#T1, $A1.#T2, $A1.#T3, $A1.#T4 $B1.#T1, $B1.#T2, $B1.#T3, $B1.#T4
  LAN Communications Controller Ports: $LAN1, $LAN2
  Expand Network Communications Lines: $<node> (e.g., where <node> = name of Remote node connected to other end of this Communication Line (i.e., JAXNDC2, JAXNDC,
  CPTMAS, NORNSC, etc.)).
  SNA (Clip1) Host Line Connection: $SNA1.#<host>
  (e.g., where <host> = name of remote host connected to the other end of this Communication Line.

- Logical Disk Volume Name Conventions

  Operating system image disk volume: $SYSTEM
  Production Disk Volumes: $PROD01, $PROD02, $PROD03
  Application Commands and User Disk Volumes: $APP01, $APP02, $APP03
  TM/MP and Safeguard Audit Trail Disk Volumes: $AUDIT1, $AUDIT2
  Development Disk Volumes: $DEV01, $DEV02, $DEV03
  Test Disk Volumes: $TEST1, $TEST2, $TEST3
  INSTALL (DSV, ISV, Database) Disk Volumes: $INST01, $INST02

- Subvolume Name Conventions

  The use of standardized naming conventions can simplify the effort required for managing Tandem systems. Using specific standardized sets of volumes, subvolumes, and file names to indicate specific functions of the data on them is helpful. For example, production data volume names could start with the five characters, $PROD, and end in a two-digit number (01-99). Subvolume names should indicate what is in them. They could start with a one-character identifier to indicate, for example, **U** for Kernel users default subvolumes, a two-character identifier to indicate an application like **AP** for accounts payable, or descriptive identifiers for system administration like TMF, EMS, BOSS, or CMON. The subvolume names should end with characters identifying what is in the subvolume. Some examples are as follows:

  - DATA
  - DICT for the DDL dictionary
  - OBJ for objects
  - SRC for source
  - LIB for application code libraries
  - CMD for command/obey files
  - PW for Pathway files

  The user subvolumes should end in their group ID and userid numbers.

  Label all volumes (except $SYSTEM) as established in conventions (e.g., execute the "PUP LABEL <$vol>,<$ldev>" for each volume where <$vol> = volume name, and <$ldev> = logical device number determined by system generation).

NOTE: Labeling a disk drive will cause all existing data on the specified drive to be erased.

Establish tape label conventions.

All tapes will be labeled with Tandem standard labels, and all tapes will be logged into a tape management system software package to ensure an auditing log of the tape media and the data that is contained on each tape. Exceptions for processing of non-standard foreign tapes will be addressed in a future release of this document.

Establish TM/MP configuration.

- Configure TM/MP to include the TM/MP control, audit dump process, backout process, **AUDITTRAIL**, **CATALOG**, **DUMPS**, **MEDIALOG**, **MEDIA** parameters and settings.

  - Number of audit trails maintained on-line for each audit trail group (prefix).

  - Assign process names for backout, audit, and dump.

  - Determine which disk volumes audit data must be logged in each Audit Trail group prefix.

  - Define the tape media information to TM/MP and initialize (label) the tape media (i.e., TMFCOM ADDTAPEMEDIA <tape volume id>,<state>).

  - Establish a location for TM/MP Audit Trail files.

  - Initialize TMF (cold start).

  - Secure all files on $SYSTEM.TMF.* using FUP as follows:

```
TACL>FUP GIVE $SYSTEM.TMF.*, 255,255
TACL>FUP SECURE $SYSTEM.TMF.*,"AGGO"
```

Establish Safeguard security control configuration.

- Configure Safeguard to provide a secure environment.

- Create ACLs for objects to be controlled.

- Establish the Kernel group IDs, userids, and related password security controls.

- Initialize Safeguard (build startup obey files [configuration, freeze user, thaw user, and other relevant obey files]).

- Verify Safeguard is properly configured by evaluating the results from the following commands:

```
TACL>SAFECOM /IN <command file below>/
= LOG <logfile (i.e., $s.#log)> ; ENV
= INFO SAFEGUARD, DETAIL
= INFO DISKFILE $DATA1.SECURE.DATA, DETAIL
= INFO DISKFILE *.*, DETAIL
= INFO DISKFILE *.*, PROGID ON, LICENSE ON
= INFO USER *.*, DETAIL
= INFO PROCESS *.*, DETAIL; INFO SUBPROCESS *.*, DETAIL
= INFO DEVICE *.*, DETAIL; INFO SUBDEVICE *.*, DETAIL
= INFO OBJECTTYPE *.*, DETAIL
= INFO GROUP *.*, DETAIL
```

- Perform the next two INFO commands using SAFECOM for each disk on the system.

```
TACL1> SAFECOM
= INFO VOLUME $DATA1, DETAIL;
= INFO SUBVOLUME $DATA1, DETAIL
= EXIT

TACL2>DSAP /OUT $S.#LOG.DSAP/ *,PROGID
```

Establish location for the system NSSQL catalog.

(i.e., SQLCI create catalog, give owner, and secure properly)

Establish tape media labeling and name conventions.

- All tapes must have an alphanumeric external sequence number, e.g.,
  - MF001 through TMF999 for TMF on-line and audit trail dump tapes
  - D00001 through D99999 for daily partial backup tapes
  - W00001 through W99999 for weekly partial backup tapes
  - M00001 through M99999 for monthly full backup tapes

- Each tape must have the same matching internal and external alphanumeric sequence number.

  - Application Subsystem Name Conventions

  - Applications must have a two-character identifier.

  - All program names in an application must start with those two characters.

  - All file names of all files owned by that application must start with those two characters.

  - All process names for programs used in this application must start with those two characters.

  - All user groupnames associated only with this application must start with those two characters.

- Process Name Conventions

  - Production processes are always named.

  - The Group Manager of the application subsystem always owns production processes.

  - Process names must be five characters or less, with the first character always **$**, the next must be the two-character application identifier, and the last two characters are variable (e.g., **$APxx** and **$PRxx**).

Establish standard file/object access levels for command-level users (user groups and userids).

- Build TACLCSTM files for users.

- Establish security measures for these userids (e.g., CMON).

- An initial password will be assigned by the IAO for the command-level userid. The user will change this password when the user initially logs on before the user can execute anything on the system.

Establish the default volume, subvolume, and file security for each user.

- (e.g., < DEFAULT $VOL.Subvol,(RWEP) >).

Establish application production database NSSQL catalogs.

(i.e., SQLCI create catalog, give owner, secure properly)

Establish non-production SQL catalogs.

(i.e., SQLCI create catalog, give owner, secure properly)

Establish administration-level Kernel (group and userids).

- Add Kernel userids and groups.
- An initial password will be assigned by the IAO for the command-level userid. The user will change this password when the user initially logs on before the user can execute anything on the system.
- Establish the default volume, subvolume, and file security for each user (e.g., < DEFAULT $VOL.Subvol,(RWEP) >).
- Establish application user/functional access matrix for each application user.

Establish application-level Kernel (user group and userids).

- Add Kernel user and group IDs.
- An initial password will be assigned by the IAO for the command-level userid. The user will change this password when the user initially logs on before the user can execute anything on the system.

Establish the default volume, subvolume, and file security for each user (e.g., < DEFAULT $VOL.Subvol,(RWEP) >).

- Establish the production database (structures, security, ownership). For each subsystem assign the tables to the appropriate catalog. Establish SQL tables and indexes.
    - Define tables, columns, etc.
    - Define table indexes.
    - Define table views (protected, etc.) for SQL table security.
    - Establish the SQL database (column, row) access rules.
    - Load data into the table.
    - Update database population statistics.
    - Test database access (queries) for functionality, optimization, etc.

Catalog all applications programs that access the SQL database to the appropriate application SQL catalog.

(e.g., SQLCOMP <program>,CATALOG <$Vol.Subvol>)

Establish application user/functional access matrix for each application user.

- Function keys should have standard assigned functions throughout all the application subsystems to minimize errors and improve user performance.

  e.g., F1 - next screen, F10 - Inquire (read)

  F11 - Add (insert/write), F12 - Update (modify/write),

  F13 – Delete (write), F16 - Back one screen, SF16 - Exit.

  The application user to function mapping could look like this:

Userid	Application	Screen Name	F1	F10	F11	F12	F13	F16	SF16
002.001	Main Router	MENU01	Y					Y	Y
002.001	AP Main	APMENU01	Y					Y	Y
002.001	AP	APEMP01	Y	Y	Y	N	N	Y	Y
002.001	AP	APEMP02	Y	Y	N	Y	N	Y	Y
002.002	Main Router	MENU01	Y					Y	Y
002.002	AP Main	APMENU01	Y					Y	Y
002.002	AP	APEMP01	Y	Y	N	N	N	Y	Y
002.002	AP	APEMP02	Y	Y	N	N	N	Y	Y
004.001	Main Router	MENU01	Y					Y	Y
004.001	AP Main	APMENU01	Y					Y	Y
004.001	AP	APEMP01	Y	Y	N	N	N	Y	Y
004.001	AP	APEMP02	Y	Y	N	Y	N	Y	Y
004.002	Main Router	MENU01	Y					Y	Y
004.003	AP Main	APMENU01	Y					Y	Y
004.002	AP	APEMP01	Y	Y	N	Y	N	Y	Y
004.002	AP	APEMP02	Y	Y	N	N	N	Y	Y

This shows that both Local User Groups 002 and 004 need to have *read* and *write* file system access to the program’s data files. The APEMP file would require its security setting to be updated to “**AAGO**”. This is because the default file access setting of “**GOGO**” would only allow the file owner’s group *read* and *execute* access.

Establish Pathway application systems (configure, startup, and build obey files).

- Build PATHMON configuration information (MAXSERVERPROCESSES, MAXSERVERCLASSES, MAXASSIGNS, MAXPARAMS, MAXPATHCOMS, MAXTERMS, OWNER, SECURITY, MAXTCPs, MAXEXTERNALTCPS, etc.).

- Build Pathway startup (cold and warm) command files.

- Build TCP configuration information.

- Build terminal configuration information.

- Build server configuration information.

- Test Pathway configuration obey files.

- Test application user/functional access.

Establish configuration and startup obey files for LAN command-level and application Windows offered to LAN users.

- Build TCP/IP and LAN configuration information (i.e., shutdown old processes first, start processes in appropriate order (LMAN, SCP, TCPIP, TELSERV, define the TLAM datalink layer, define the Windows for TELSERV, LISTNER, etc.). Test the TCP/IP LAN startup obey files.

- Build and test the startup obey files for the Pathway application interface.

- Test user (command-level and Pathway) access through the LAN (i.e., all TCP/IP restriction parameters to the Tandem LAN interface must be defined in the TLAM datalink layer configuration obey file for definition to TCPIP).

- The following example allows two LAN interfaces with a specific IP address (LAN network interface type card access) with subnet masking and default static route statement for each connection.

- This example also demonstrates the authorized Tandem services for access over the LAN. This is in the form of an SCF (Subsystem Control Facility) input command file executed from TACL with an "SCF/IN <command file>/" command.

```
ALLOW          ALL
ASSUME         LINE $LAM1
PRIMARY        LINE $LAM1, 3
START          LINE $LAM1, SUB ALL

ABORT          PORT *
DELETE         PORT *
ADD            PORT #IP, TYPE ETHERNET, ADDRESS %h800, &
               DATAFORWARDTIME 0.02, DATAFORWARDCOUNT 4
ADD            PORT #ARP, TYPE ETHERNET, ADDRESS %h806, &
               DATAFORWARDTIME 0.02, DATAFORWARDCOUNT 4
START          PORT *

ASSUME         PROCESS $ZTC1
ADD            SUBNET #TNDM, TYPE ETHERNET, DEVICENAME $LAM1,
               IPADDRESS 192.42.80.62
ALTER          SUBNET #LOOP0, IPADDRESS 127.1
ADD            ROUTE #GT01, DESTINATION 0.0.0.0, GATEWAY
               192.42.80.1
START          SUBNET *

START          ROUTE *

ASSUME         LINE $LAM2
PRIMARY        LINE $LAM2, 6
START          LINE $LAM2, SUB ALL

ABORT          PORT *
DELETE         PORT *
ADD            PORT #IP, TYPE ETHERNET, ADDRESS %h800, &
               DATAFORWARDTIME 0.02, DATAFORWARDCOUNT 4
ADD            PORT #ARP, TYPE ETHERNET, ADDRESS %h806, &
               DATAFORWARDTIME 0.02, DATAFORWARDCOUNT 4
START          PORT *

ASSUME         PROCESS $ZTC2
ADD            SUBNET #TNDM, TYPE ETHERNET, DEVICENAME $LAM2,
               198.49.123.62
```

```
    ALTER               SUBNET  #LOOP0, IPADDRESS 127.1
    ADD                 ROUTE #GT01, DESTINATION 0.0.0.0, GATEWAY
                        198.49.123.1

    START               SUBNET *
    START               ROUTE *
```

All services to be provided to the LAN users must be defined in the Windows configuration obey file for definition to TELSERV. The following example allows for three types of access over the LAN (BOSS, a Pathway-type access, BOSS2, a Pathway test type of access, and [space], a non-displayed choice of print-type service).

***NOTE*:** TELSERV will be started with the parameter **NOTACL** to prevent the full TACL access from being available to the LAN users. This can be done by using the following command, but it must be done before adding Windows:

```
RUN $SYSTEM.SYSTEM.TELSERV/NAME $ZTN0/ -NOTACL
```

This set of commands could be stored in the form of an SCF input <command file> executed from TACL with a "SCF/IN <command file>/" as an example.

```
ALLOW ALL
ASSUME PROCESS $ZTN0
ALTER MAXTERMINALS 128

ADD WINDOW $ZTN0.#WIN01, SERVICENAME "BOSS", SERVICETYPE BLOCK
ADD WINDOW $ZTN0.#WIN02, SERVICENAME "BOSS", SERVICETYPE BLOCK
ADD WINDOW $ZTN0.#WIN03, SERVICENAME "BOSS", SERVICETYPE BLOCK
ADD WINDOW $ZTN0.#WIN04, SERVICENAME "BOSS", SERVICETYPE BLOCK
ADD WINDOW $ZTN0.#WIN05, SERVICENAME "BOSS2", SERVICETYPE BLOCK
ADD WINDOW $ZTN0.#WIN06, SERVICENAME "BOSS2", SERVICETYPE BLOCK
ADD WINDOW $ZTN0.#PTR1, SERVICENAME " ", SERVICETYPE PRINT

START WINDOW $ZTN0.*
```

NOTE: TCP/IP services can be limited using the command input configuration files (**PORTCONF**, **HOSTS**, and **SERVICES**) to define how they are run.

- Implement all conventions that were established.

- Verify that all security is set appropriately.

```
        TACL1>DSAP *, PROGID, LICENSED
```

APPENDIX D. "HOW TO" GUIDE FOR TANDEM (NSK)

DEVELOPER: Accelerate software for RISC processors.

NOTE**:** This function should be performed by CDA personnel only.

```
TACL>LOGON SUPER.SUPER,<pswd>
TACL>AXCEL /IN $<object_vol>.<objsubvol>.<program_obj>/
TACL>LOGOFF
```

This is only necessary if the Tandem site is executing on a RISC processor type and the application software was not developed on a native RISC system. The application software performance usually improves after the AXCEL tool is executed against the object programs to convert the program from using the CISC instructions to the RISC instruction set.

EXPAND: Address EXPAND network security issues.

All command-level users are implicitly denied access across the EXPAND network unless specifically allowed access by the **REMOTEPASSWORD** command and by the Kernel file system file access security settings. Command-level users who need EXPAND network access must have their remote passwords established and then only for the nodes to which they need access. Only files and programs that need to be accessed over the network must have remote network file access security.

INSPECT: Remove the Inspect debugging tool parameters stored with an object program, and then secure the old program away from all users except the local SUPER.SUPER userid.

These Inspect parameters are used for program debugging to display data that is being processed by the program:

```
TACL> LOGON SUPER.SUPER (or userid with read, write, purge access to object file)
TACL> BIND
@ ADD CODE $<object_vol>.<object_subvol>.<program_obj>
@ STRIP
@ BUILD & $<object_vol>.<NEW_objsubvol>.<program_obj>
@ EXIT
TACL>RENAME $<object_vol>.<object_subvol>.<program_obj>, &
    $<object_vol>.<OLD_object_subvol>.<program_obj>
TACL>RENAME $<object_vol>.<NEW_objsubvol>.<program_obj>,&
    $<object_vol>.<object_subvol>.<program_obj>
TACL>FUP SECURE $<objvol>.<OLD_objsubvol>.<program_obj>,-1
```

KERNEL: Implement Kernel Enscribe file security.

The established file security settings depend on several factors. The determining factors are as follows:

- The level of access (*read*, *write*, *execute*, *purge*, *create*, and *owner*) required by all users and processes that are authorized access)

- The sensitivity of the data stored in the file

- Whether the access is from local and/or remote Tandem node(s)

- How many users of the same or different Kernel groups (application subsystems and user groups) require access to the data

FUP SECURE files.

FUP SECURE the files as appropriate (e.g., files that do not have any need to be accessed outside of this application could be set to **$Volume.Subvol.File,"GOGO"**).

Files that do have a need to be accessed outside of this application, and do not have a need to be secured from the rest of the users on the local Tandem system could have their security set using FUP SECURE as appropriate (e.g., set to **$Volume.Subvol.File,"AOGO"**).

Files that have access needs that span outside the normal Enscribe security measures should be addressed with Safeguard. Some examples are below:

- Files that have a need to be accessed outside of this application, and a need to be secured from the rest of the users on the local Tandem system should have their security set through a Safeguard ACL declaring as an object the **$Volume.Subvol.File**. The set of users (groups) that needs access should have access permissions set appropriately (read, write, create, purge, and owner) and each should have an ACL record added to allow access to this file.

- Files that have a need to be accessed by only some specific users on remote nodes and only some specific local users that are outside of this application user group with a need to be secured from the rest of the local and remote Tandem users. These files should have their security set through a Safeguard ACL declaring the **$Volume.Subvol.File** as an object. The set of users (groups) who need access should have access permissions set appropriately (*read*, *write*, *create*, *purge*, and *owner*) and each should have an ACL record added to allow access to this file.

KERNEL: Implement Kernel userids (group and user) in Safeguard and TACL.

Log on to the administrative group userid:

SAFEGUARD

```
TACL>SAFECOM
= ADDUSER <group.user for each userid>, <group#>, & <userid#>, default <default
Volume.svolume>, <security>, & <password restrictions>… etc.
```

TACL

```
LOGON group1.user1,password (creates default TACLCSTM)
PASSWORD group1.user1 (set default password)
DEFAULT $<Volume>.<Subvolume>,"OOOO"
```

KERNEL: Implement Kernel userids (group and user) in TACL and BOSS.

TACL

```
TACL1>LOGON SUPER.SUPER
TACL2>ADDUSER <GROUP>.<USERID>,<GROUP#>,<USERID#>
TACL3>LOGON <GROUP>.<USERID>
TACL4>PASSWORD <new password>
TACL5>DEFAULT <default Volume.Subvolume>, "OOOO"
TACL6>LOGOFF
```

BOSS

See *Section C.2, How to Add Users/Applications,* of the *BOSS Block-mode Operating System Services User's Guide*, *Version 4.0K*.

TACLLOCL, TACLCSTM files, and TACL macros (other tools like SCF that support the CSTM files) need to be pre-established if specific functions need to be controlled or set up for these tools.

- Design, develop, and test appropriate TACL macros required by users.

- Create TACLCSTM files with appropriate commands to establish the appropriate set of default TACL macros for the user.

Example:

```
?TACL MACRO
== TACL created this file for your protection.
#SET #INFORMAT TACL
SETPROMPT BOTH
LOAD/KEEP 1/<macros>
```

NOTE: The **macros** will be a file that consists of macros the user frequently uses.

- Create a SCFCSTM file and load with appropriate commands to establish the appropriate set of SCF defaults for the user.

NOTE**:** Please refer to the *Subsystem Control Facility Reference Manual*, *Section 2*, *Operating SCF*, under the heading of *SCF Custom File* for an example. This example is found in the *Total Information Manager CD "D39.0 to D39.01.***"**

PATHWAY: Address Pathway security considerations (servers, TCPs, terminals, and external calls).

Configure the PATHMON owner and default security.

Control user PATHCOM access from command-level prompts.

Control user access through BOSS menus and submenus.

Permit external client calls to Pathway servers through the use of LINKMON.

Remote procedure call provides access to open systems clients.

PRIVILEGED PROGRAMS: How to check for privileged programs.

Before you check the programs to see if they contain privileged code, a list of programs (100 & 700) can be obtained by using DSAP & ENFORM. Using the following, a temporary file containing the files and related information can be created, if not already present. Ensure that the DSAPWORK file is current. If this file is not current purge the file and issue the following command:

```
DSAP *,WORKFILE DSAPWORK
```

Once the DSAPWORK file has been created, use ENFORM and the DSAPDDL to produce a report for all code 100 and code 700 files. The list can then be used to check each file for privileged code.

```
?DICTIONARY SRRLIB;
?ASSIGN DSAP-RECORDI, DSAPWORK
```

```
OPEN DSAP-RECORDI

SET @SPACE TO 1;

LIST

     ASCD   FILE.FILENAME     NOPRINT

     FILE.VOLUME
     FILE.SUBVOLUME
     FILE.FILENAME
     OWNERREDEF.GROUP
     OWNERREDEF.USER
     FILECODE               HEADING "FILE/CODE"
     SECURITY.READ          HEADING "R"
     SECURITY.WRITE         HEADING "W"
     SECURITY.EXECUTE       HEADING "E"
     SECURITY.PURGE         HEADING "P"
     AUDITED                HEADING "A"
     LICENSED               HEADING "L"
     PROGID                 HEADING "P"
WHERE
     FILECODE = 100 OR
     FILECODE = 700
;
```

Using the NOFT application you can get information about files that are code 700 files. The following are commands to get information about code 700 files.

```
> FILEINFO ZSTFNSRL

                  CODE          EOF   LAST MODIFIED  OWNER  RWEP
ZSTFNSRL  O    700          126088 12AUG2002 13:31   255,255    ****
```

```
> NOFT
NOFT> FILE ZSTFNSRL
NOFT> LISTATTRIBUTE

                   Object File : <NODE>.$SYSTEM.SYS04.zosscsrl
                   File Format : ELF
                     Timestamp : 2002 August 12, 13:08:39
      Symbols/INSPECT Region : Yes
                   System Type : Guardian
                    Executable : Yes
               Process Subtype : 0
                Highrequesters : Yes
                      Runnamed : No
                       Highpin : Yes
                     Saveabend : No
              Priv or Callable : No
                      Callable : No
               DEBUG/INSPECT : INSPECT
             Maximum Heap Size : 0
               Main Stack Size : 0
               Space Guarantee : 0
                      PFS Size : 0
                   Fingerprint : 0000-0000-0000-0000
           Fingerprint Version : 0
                   Ctors_vaddr : 0x00000000
                   Dtors_vaddr : 0x00000000
                   Initz_vaddr : 0x00000000
                   Termz_vaddr : 0x00000000
   Directly Needed Public SRLs : 0
Directly Needed Public SRL Bitmap : 0x0000 0x0000 0x0000 0x0000 0x0000 0x0000
0x0000 0x0000
                      SRL Name : ZOSSCSRL
             SRL Export Digest : 8fcd75186127f3f21ef68e50379037b1
              SRL Text Address : 0x76200000
              SRL Data Address : 0x58080000
      SRL Entry Vector Address : 0x79f80000
  SRL Export Entry Vector Size : 64
                    SRL Client : Yes
           Floating-Point Type : TANDEM_FLOAT
             Float-lib-overrule : No
                   MCB address : not available
```

From the above information, to see if this licensed program has privileged code, you need to see if the “Executable” and “Priv or Callable” parameters are set to Yes.

```
Select the topic desired by typing "HELP <topic>"

<topic> is:

COMMENTDUMPADDRESSDUMPOFFSET
DUMPPROCENVEXITFC
FILEHELPHISTORYLAYOUT
LISTATTRIBUTELISTCOMPILERSLISTOPTIMIZELISTPROC
LISTSOURCELISTSRLINFOLISTSRLEXPORTSLISTSRLFIXUPS
LISTUNRESOLVEDLISTUNREFERENCED LOGOBEY
OUTRESETSET CASESET FORMAT
SET HISTORYBUFFER SET HISTORYWINDOW SET LINES SET LOG
SET OUTSET SCOPEPROCSET SCOPESOURCE SET SORT
SHOWSYSTEMVOLUMEXREFPROC
Allcommandscommand_lineobject_files
Proceduresshortcutssource_files
```

```
> FILEINFO SCP

          CODE          EOF   LAST MODIFIED  OWNER  RWEP
SCP       O    100PL      554046 25SEP2002  8:55 255,255 UUCU

>BIND
@LMAP FROM SCP

TIMESTAMP  24MAR02 20:04:50

SP  PEP  BASE    LIMIT   ENTRY   ATTRS    NAME

00  314  177522  177522  177522         APPL^ABEND
00  226  143536  143560  143536         APPL^AWAITIOX
00  006  004154  004272  004154         APPL^BACKUPSTART
00  007  004273  004411  004273         APPL^BACKUPSTOP
00  246  157707  160605  160006  EV     APPL^DOCHECKPOINT
01  007  003157  003160  003157         APPL^EMSCHANGED
00  013  005435  005542  005435         APPL^EXECUTE
00  004  001630  002623  001630         APPL^INITIALIZE
00  014  005543  005740  005543         APPL^IO^BUFFER^OFFSETS
01  050  020760  020761  020760         APPL^MEMORYALERT
00  260  164077  164077  164077         APPL^MEMORYTRACE
00  316  177535  177535  177535         APPL^NOTECPUCHANGE
00  261  164100  164555  164353         APPL^NOTEEVENTV
00  317  177536  177536  177536         APPL^PROCESSBREAKMESSAGE
00  015  005741  006177  005741         APPL^PROCESSCANCEL
00  016  006200  006501  006200         APPL^PROCESSCLOSE
00  017  006502  006726  006502         APPL^PROCESSDEVICEINFO
```

```
01  042  015772  016047  015772         APPL^PROCESSFILENAMENEXT
00  037  034663  043211  042310         APPL^PROCESSIOREQUEST
00  020  006727  007457  006727         APPL^PROCESSOPEN
00  005  002624  004153  003100         APPL^PROCESSSTARTUP
00  262  164556  164567  164556         APPL^PUTSUBJECTNAME
00  236  144520  144520  144520         APPL^RECOVERCHCB
00  021  007460  007604  007460         APPL^RECOVEROCB
00  042  052352  052566  052352         APPL^SPIR^CALIBRATE
00  043  052567  053407  052567         APPL^SPIR^CLEANUP
00  306  171547  171547  171547         APPL^SPIR^INITIATE^DELAY
00  044  053410  053534  053410         APPL^SPIR^NULLOBJECTNAME
00  036  022547  034662  033665         APPL^SPIR^PERFORM
00  045  053535  053702  053535         APPL^SPIR^STEPLEAF
00  040  043212  047520  047161         APPL^SPIR^STEPROOT
00  046  053703  054435  053715         APPL^SPIR^STOREQUALIFIERS
01  065  025000  025001  025000         APPL^SPIR^VALIDATERULE
00  174  135070  135153  135070         APPL^SYSGENEDINITIALIZE
01  136  053727  053730  053727         APPL^TESTPOINT
01  144  055315  055316  055315         APPL^TRACE^HEADER^SIZE
01  145  055317  055317  055317         APPL^TRACE^START
00  320  177537  177537  177537         APPL^TRACE^STOP
01  100  034770  037374  036044  V      CHARMAP_GET_
00  052  061314  061562  061320         FILENAMETOPROCESSHANDLE
00  321  061563  061764  061563  PC     GETBACKUPINFO
00  034  017231  017612  017231         GETPAID
00  153  130062  130175  130062         KP^ABEND
01  016  005665  006176  006115  V       KP^ALLOCATESEGMENT
00  245  157707  160605  160004  V       KP^APPL^DOCHECKPOINT
01  032  011640  015252  013642          KP^BASEINITIALIZE
00  202  140167  140447  140274  V       KP^CALL
00  315  177523  177534  177523          KP^CHECKCLOSE
01  004  002662  003063  003044          KP^CHECKOPEN
01  053  022611  022650  022611  V       KP^CHECKPOINTCHCB
01  027  010540  010557  010540          KP^CHECKPOINTOCB
00  270  165616  165652  165616          KP^CHILDDEREGISTER
00  111  115711  116070  115711  V       KP^CHILDSTOP
00  104  113535  113777  113535          KP^COPYERRORLIST
00  074  104501  111051  110545  V       KP^CYCLELOOP
00  073  100000  104500  104117  V       KP^CYCLESTARTUP
00  164  132272  132771  132314          KP^DEFINEADDMAP
00  150  127226  127272  127226          KP^DELINK
01  143  055033  055314  055033  V       KP^DEVICEINFO
00  140  125242  125331  125242          KP^DEVICEINFONOWAIT
01  024  007773  010300  010233  V       KP^DROPOPENER
01  013  004752  005073  004752  V       KP^EL^ALLOCATESEGMENT
01  010  003161  003650  003205  V       KP^EL^PROCESSCREATE
```

```
00  142  125613  125671  125613         KP^ERRORLISTBEGIN
00  145  126740  126750  126740         KP^ERRORLISTEND
00  313  177512  177521  177512         KP^ERRORLISTPOP
00  144  126127  126737  126443  V      KP^ERRORLISTPUSH
00  143  125672  126126  125672  V      KP^ERRORLISTPUT
01  075  034311  034466  034311  V      KP^ERRORLISTPUTFNAME
00  112  116071  116334  116071  V      KP^ERRORLIST^ZFIL
00  113  116335  116353  116335  V      KP^ERRORLIST^ZGRD
00  114  116354  116447  116354  V      KP^ERRORLIST^ZSPI
00  233  144100  144331  144100  V      KP^EVMINITIALIZE
00  163  132264  132271  132264         KP^FILECLOSE
01  141  054172  054725  054172  V      KP^FILECREATE
00  155  130766  131001  130766         KP^FILEERROR
01  006  003105  003156  003105         KP^FILEGETNAME
01  076  034467  034654  034467  V      KP^FILEMODTIME
00  123  116664  120625  120524  EV     KP^FILENAMETOFNAME32
00  120  116664  120625  120463  EV     KP^FILENAMETOINTERNAL
00  121  116664  120625  120476  EV     KP^FILENAMETOLOCAL
00  122  116664  120625  120511  EV     KP^FILENAMETONETWORK
00  117  116664  120625  120424  V      KP^FILENAMETOSTRING
00  271  165653  166505  165653  V      KP^FILEOPEN
01  142  054726  055032  054726         KP^FILEPURGE
01  033  015253  015416  015253         KP^FINDFILE
00  217  142753  142766  142753         KP^FIXEDSTATPRESET
00  242  157432  157450  157432         KP^FREEQUEUE
00  254  161673  162460  162420  E      KP^GETBUFFERTAGGED
00  067  077535  077604  077555  E      KP^GETBUFFERTAGGEDORDIE
00  065  076037  077534  076454         KP^GETMEMORYTAGGED
00  066  077535  077604  077540         KP^GETMEMORYTAGGEDORDIE
01  051  020762  021105  021001  V      KP^GETMESSAGE
01  106  040722  044216  043066         KP^GETMESSAGEV
00  167  133437  133661  133437         KP^GETRECEIVEINFO
01  077  034655  034767  034655         KP^GETSEGMENTID
00  102  113135  113364  113135  V      KP^GUARDIANERROR
00  151  127273  127426  127273         KP^IFREMOTENAME
00  101  113072  113134  113072  V      KP^IFSAMEOPENER
00  156  131002  131041  131002         KP^IFSAMEPROCESS
00  077  112616  112716  112616  V      KP^INTERNALERROR
00  216  142722  142752  142722  V      KP^INTSTATPRESET
00  135  123071  123130  123071         KP^ISMYPROCESSNAME
00  231  143743  144051  143743         KP^MAXTABLESIZE
00  234  144332  144441  144332  V      KP^NEXTOCB
00  214  142577  142647  142577  V      KP^NOTEALLOCATESEGMENTERROR
00  107  114366  114601  114424  V      KP^NOTEEVENT
00  146  126751  127155  126751  V      KP^NOTEIOERROR
01  012  004077  004751  004123         KP^NOTENEWPROCESSERROR
```

```
00  075  111052  111345  111115  V       KP^NOTEPROCESS
00  103  113365  113534  113365  V       KP^OPENERHANDLE
00  071  077646  077735  077646          KP^OPENERNAME
00  220  142767  143015  142767          KP^OPENERNODE
00  134  122762  123070  122762          KP^OPENERPAID
00  160  131055  131404  131055  V       KP^OPENRECEIVE
01  026  010334  010537  010334  V       KP^PARSEHANDLE
01  072  025506  025661  025646  V       KP^PATTERNMATCH
01  036  015651  015703  015651          KP^POPBOTTOM
00  106  114336  114365  114336          KP^POPTOP
00  212  142403  142414  142403          KP^PRESETQUEUE
01  011  003651  004076  003651  V       KP^PROGRAMFILEINFO
00  241  157357  157431  157357          KP^PUSHBOTTOM
00  147  127156  127225  127156          KP^PUSHTOP
00  076  111346  112615  111346          KP^PUTMEMORY
00  105  114000  114335  114000  V       KP^QUEUEREPLY
00  116  116551  116663  116551  V       KP^ROB^DEQUEUE
00  124  120626  121053  120626  V       KP^ROB^FILEOPEN
01  140  053731  054171  054102  EV      KP^ROB^FILE^CONTROL
01  137  053731  054171  053736  V       KP^ROB^FILE^SETMODE
00  273  166654  166766  166654          KP^ROB^MESSAGE^REPLY
00  110  114602  115710  114733  V       KP^ROB^MESSAGE^SEND
01  114  046024  046077  046024          KP^ROB^NEXTTHCB
01  003  002456  002661  002456          KP^ROB^READY
00  141  125332  125612  125443          KP^ROB^READYORTIMEOUT
00  137  124634  125241  124634          KP^ROB^START
01  014  005074  005104  005074          KP^SAVECHECKPOINT
00  057  074515  075242  075201          KP^SAVECHECKPOINTBYTES
00  250  161175  161435  161216          KP^SCANFIXED
00  170  133662  134511  134460          KP^SCANFNAME
00  064  075771  076036  075771          KP^SCANINT
00  172  134555  134661  134555          KP^SCANNAME
00  173  134662  135067  134662          KP^SCANTRUTH
00  171  134512  134554  134512          KP^SCANUINT
00  166  132772  133436  133426  EV      KP^SETEMSFILE
00  165  132772  133436  133416  V       KP^SETLOGFILE
01  113  045755  046023  045755          KP^SETMSGFILE
00  267  165554  165615  165554  V       KP^SETUPCHCB
00  204  140517  141314  140517  V       KP^SETUPDATASEGMENT
00  100  112717  113071  112717  V       KP^SETUPOCB
00  161  131405  132156  132005  V       KP^SHIFTSTRING
01  115  046100  046212  046100  V       KP^SPIR^BEGINSEGMENT
00  277  167347  170043  167432  V       KP^SPIR^COMMITTED
01  124  050510  050653  050543          KP^SPIR^ENDSEGMENT
00  130  121147  121254  121147  V       KP^SPIR^E^GENERIC
01  064  024732  024777  024732  V       KP^SPIR^E^SPI^ERR
```

```
01  057  023164  023345  023164  V      KP^SPIR^E^TKN^XXX
00  131  121255  121536  121255  V      KP^SPIR^E^ZFIL
01  112  045475  045754  045475  V      KP^SPIR^GETTOKEN
00  136  123131  124633  123150         KP^SPIR^INITIATE
00  133  122730  122761  122730         KP^SPIR^NOTEREPLIED
01  066  025002  025146  025002  V      KP^SPIR^NOTESPIEVENT
01  116  046213  047442  046222  V      KP^SPIR^PUTANSWER
01  117  047443  047651  047443  V      KP^SPIR^PUTCHARMAPINFO
01  135  053633  053726  053633  V      KP^SPIR^PUTFILEINFO
01  120  047652  047756  047660         KP^SPIR^PUTFIXEDSTAT
01  121  047757  050054  047757         KP^SPIR^PUTGATESTATS
01  122  050055  050204  050063         KP^SPIR^PUTINTSTAT
01  123  050205  050507  050342         KP^SPIR^PUTOPENER
00  132  121537  122727  122501  V      KP^SPIR^PUTTOKEN
00  126  121067  121100  121067         KP^SPIR^PUTTOKENINT
00  127  121101  121146  121101         KP^SPIR^PUTTOKENMAPPED
00  300  170044  170222  170044  V      KP^SPIR^PUTTOKENNAME
01  063  024565  024731  024565         KP^SPIR^SETUPTOKEN
00  275  167033  167307  167033  V      KP^SPIR^STARTERROR
01  062  024544  024564  024544         KP^SPIR^TOKENMISSING
00  125  121054  121066  121054         KP^SPIR^TOKENOCCURS
00  062  075243  075605  075577  E       KP^SPI^CLEARTABLE
00  305  171332  171546  171332         KP^SPI^CLOSETABLE
01  134  053454  053632  053565         KP^SPI^FINDDECODE
00  061  075243  075605  075572  E       KP^SPI^NULLTABLE
00  060  075243  075605  075570         KP^SPI^OPENTABLE
01  056  023020  023163  023020         KP^SPI^SETUPDECODE
00  070  077605  077645  077605         KP^TESTMEMORYTAGGED
00  072  077736  077777  077736         KP^TIMECANCEL
00  063  075606  075770  075606  V      KP^TIMERECALL
01  127  053162  053225  053162         KP^TIMESTAMPTOJULIAN
00  215  142650  142721  142650         KP^TIMESTATPRESET
00  225  143420  143535  143420         KP^TIMESTATSET
01  044  016170  016216  016170         KP^TMF^RESUME
00  243  157451  157463  157451         KP^TOP
00  257  163416  164076  163673         KP^TRACE^GETADDRESS
01  126  051124  053161  051217         KP^TRACE^START
00  247  160606  161174  160606         KP^TRACE^STOP
00  162  132157  132263  132157         KP^UNQUOTESTRING
01  110  044531  044677  044536  V      KP^WRITEEMS
00  252  161515  161672  161515         KP^WTOLINE
00  205  141315  141602  141331        KP^XLATE^INIT
01  020  006275  006727  006275        KP^XLATE^LOCATE
01  054  022651  022754  022651        KX^ADDOPENNOWAIT
01  015  005105  005664  005105        KX^ADDPOOLSECTION
00  221  143016  143150  143016        KX^ADJUSTMONITORNET
```

```
00  154  130176  130765  130711        KX^ARMTRAP
00  177  135415  137736  137532        KX^BACKUPFSM
00  200  137737  140136  137737        KX^BACKUPNOTIFY
00  251  161436  161514  161436        KX^CATALPHA
00  302  170373  170456  170373        KX^CATENUM
01  035  015524  015650  015524        KX^CATHEXVALUES
00  264  165224  165345  165224        KX^CATPROCESSNAME
01  132  053227  053365  053227        KX^CATSSID
00  152  127427  130061  127427  V     KX^CATVALUE
01  005  003064  003104  003064        KX^CHECKPOINTBYTESNOW
01  055  022755  023017  022755        KX^CHECKPOINTSIZE
01  023  007372  007772  007432        KX^CHILDNOTIFY
00  266  165472  165553  165472  V     KX^CHILD^IDTOINDEX
00  201  140137  140166  140137        KX^CHILD^INDEXTOID
00  175  135154  135222  135154        KX^CYCLEINITIALIZE
00  230  143661  143742  143661        KX^DELOPENNOWAIT
01  031  010611  011637  011433        KX^EVM^DEFINETEMPLATE
00  301  170223  170372  170223  V     KX^GETPINFO
00  253  161673  162460  162250        KX^GETREGIONTAGGED
01  103  037443  037630  037443        KX^IFSYSGEN
00  176  135223  135414  135277        KX^ISOLATEBACKUP
00  240  156456  157356  157012        KX^ISSUEREPLY
00  255  162461  162573  162461        KX^MEMORYDIAGNOSE
01  047  017161  020757  017560  V     KX^MEMORYTRACE
01  105  040573  040721  040573        KX^MEMORYVALIDATE
00  256  162574  163415  162574        KX^MEMORY^CHECK
00  203  140450  140516  140450        KX^MEMORY^PRESETPOOL
00  210  142100  142362  142227        KX^NOTECPUCHANGE
01  041  015754  015771  015754        KX^NOTENODEDOWN
00  206  141603  141647  141603        KX^PREPAREDISPTRACE
01  111  044700  045474  045312  V     KX^PRINTEMS
00  222  143151  143247  143151        KX^PROCESSHASH
01  133  053366  053453  053366        KX^PURGEMESSAGES
00  263  164570  165223  164570        KX^PUTREGION
00  224  143315  143417  143315  V     KX^READRECEIVE
00  157  131042  131054  131042        KX^RECEIVEDEPTHMAX
00  237  144521  156455  155773        KX^RECEIVEDONE
01  037  015704  015732  015704        KX^RECOVERABLE^BEGIN
01  040  015733  015753  015733        KX^RECOVERABLE^END
01  025  010301  010333  010301        KX^RECOVERABLE^TEST
00  223  143250  143314  143250        KX^RETURNOCB
00  235  144442  144517  144442        KX^ROB^CHILD^DONE
01  043  016050  016167  016050        KX^ROB^CLEANUP
00  244  157464  157706  157464        KX^ROB^EXECUTE
00  211  142363  142402  142363        KX^ROB^INITIALIZE
00  115  116450  116550  116450        KX^ROB^IO^DONE
```

```
00 265 165346 165471 165346     KX^ROB^TESTEXECUTE
00 312 177470 177511 177470     KX^ROB^TIMEWAKE
00 272 166506 166653 166512 V   KX^ROB^WAITFORALERT
00 213 142415 142576 142415     KX^SEGMENT^RECORDORIGIN
01 052 021106 022610 022303 V   KX^SENDEMS
00 207 141650 142077 141650     KX^SETADDRESSES
00 232 144052 144077 144052     KX^SETBACKUP
01 107 044217 044530 044217     KX^SETFORMATPARAMS
01 067 025147 025203 025147     KX^SPIR^BEGINOBJECT
00 307 171550 176011 173414     KX^SPIR^CHECK
01 070 025204 025401 025204     KX^SPIR^CLEANNAME
01 002 000467 002455 001046     KX^SPIR^DOCOMMAND
00 311 177450 177467 177450     KX^SPIR^ENDOBJECT
01 060 023346 023404 023346     KX^SPIR^FINDOTYPE
00 303 170457 171006 170457     KX^SPIR^GETCONTEXT
01 061 023405 024543 023405     KX^SPIR^GETOBJECT
00 310 176012 177447 177442     KX^SPIR^NEXTOBJECT
00 304 171007 171331 171007     KX^SPIR^PUTCONTEXT
01 073 025662 026010 025662     KX^SPIR^REPOSITION
00 274 166767 167032 166767     KX^SPIR^SETBUFFERFULL
01 071 025402 025505 025402     KX^SPIR^TRACEITEM
01 074 026011 034310 033722     KX^SPIR^UNDERSTAND
00 276 167310 167346 167310     KX^SSPUTLONG
01 125 050654 051123 050701     KX^TESTPOINT
00 227 143561 143660 143561     KX^TMF^IO^DONE
01 104 037631 040572 037701     KX^TMF^STATECHECK
01 030 010560 010610 010560     KX^TMF^TAGTEST
01 034 015417 015523 015417     KX^TOTALNOWAITDEPTHUPDATE
01 046 016573 017160 016573     KX^TRACE^IO^DONE
01 017 006177 006274 006177     KX^TRACE^SETUP
01 045 016217 016572 016443     KX^TRACE^SHUTDOWN
01 101 037375 037442 037400     KX^VERSIONPROC
01 130 053226 053226 053226     KX^VERSIONT9112PROC
01 022 007032 007371 007074 V   KX^XLATE^ATTACH
01 021 006730 007031 006730     KX^XLATE^SETFILE
00 050 054762 060416 056550     RETRY
00 003 000470 001627 001473 M   SCP
00 023 012620 014042 013100 V   SCP^BADSERVER
00 026 014350 014775 014350     SCP^CLOSESERVER
00 027 014776 015566 014776     SCP^CMDTIMEOUT
00 030 015567 016030 015567     SCP^DEVINFO^DONE
00 056 070454 074514 074055     SCP^DOTRACINGTH
00 047 054436 054761 054436 V   SCP^ERRORLIST^ZFIL
00 022 007605 012617 011301 V   SCP^ERRREPLY
00 025 014205 014347 014205     SCP^GENERATE^POOL^FULL^EVT
00 010 004412 004531 004412     SCP^GETMEMORY
```

```
00  011  004532  004651  004532         SCP^GETMEMORYORDIE
00  024  014043  014204  014043         SCP^IS^SPI^BUFFER
00  035  017613  022546  022027         SCP^OPENSERVERTH
00  053  061765  065761  065402         SCP^PROCESSEDBYTRACE
00  012  004652  005434  004652         SCP^PUTMEMORY
00  031  016031  016162  016031         SCP^SENDDELAYED
00  051  060417  061313  060417         SCP^SERVERRECEIVE
00  041  047521  052351  051732         SCP^SERVERSEND
00  032  016163  017077  016360         SCP^SERVTIMEOUT
00  033  017100  017230  017100         SCP^SHUTDOWN
00  054  065766  067704  067534         SCP^TRACEINITIATE
00  055  067705  070453  067705         SCP^TRACEMODIFY
00  322  065762  065765  065762  PC     SWITCHUSER^
01  102  037375  037442  037402  E     T6563D40^29APR1999^T09K^ABK
01  131  053226  053226  053226  E     T9112D40^28APR1999^V55ACW
00  002  000467  000467  000467        T9395G05^06APR02^25MAR02^ACC  011235  P
    vsprintf
```

In the ATTRS column, if there is a "P" or "C" then the object is privileged.

For users to execute a program in privileged mode, the program has to be licensed, with one exception. The only userid on the system that can run privileged code, without being licensed, is the SUPER.SUPER userid. Because of the ability of the SUPER.SUPER ID, all 100 and 700 files will be checked on the system in accordance with the above.

```
Help is available on these BINDER commands and topics:

ADD               ALTER             Attributes         Binder
block-list        block-name        block-range         BUILD
CD                CHANGE            CLEAR               Commands
COMMENT           Control-Lists     DELETE              DUMP
entry-list        entry-name        entry-range         ENV
Error             EXIT              FC                  FILE
HELP              HIGH-PIN          INFO                LIST
LMAP              LOG               MODE                MODIFY
MOVE              name-list         OBEY                OUT
RENAME            REPLACE           RESELECT            RESET
SATISFY           SELECT            SET                 SHOW
String            STRIP             SYSTEM              VERIFY
VOLUME
```

REMOTE ACCESS: Implement Kernel remote Enscribe file access.

- Only data files that need EXPAND network access must have their file security (*read*, *write*, *execute*, and *purge*) set for remote access as follows:

- **N** Network anyone
- **C** Network community or group
- **U** Network user

Care needs to be taken to ensure access is set to the appropriate level. An example would be for a file the IAO determines to allow any user on remote nodes to have *read* access only. Then the **READ** parameter would have the value set to **N** for anyone on any node. If the IAO determines to allow any user in the same Kernel group on remote nodes to have *write* access, only then would the **WRITE** parameter have the value set to **C** for anyone in the file owner's Kernel group on any node. If the IAO determines to allow any user with the same Kernel group and userid on remote nodes to have *execute* access, only then would the **EXECUTE** parameter have the value set to **U** for anyone with the same Kernel group and userid as the file owner on any attached node with remote passwords that are correctly set.

Please note that file security for the remote access level settings is not node specific (all nodes that are set up properly are included). Also note that users without network access cannot access files on other nodes no matter to what the file security is set.

REMOTE ACCESS: Implement Kernel remote passwords.

NOTE: Both of the **REMOTEPASSWORD** commands below will be executed in exactly the same syntax at each of the two nodes to which the user wants access.

After logging into **ADMIN.SM1**, issue the following commands:

```
RPASSWRD \JAXNDC2,<JAXNDC2Password>
RPASSWRD \CPTMAS,<CPTMASPassword>
```

SAFEGUARD: Implement Safeguard userid password change security.

```
TACL> SAFECOM

= ALTER SAFEGUARD, PASSWORD-REQUIRED ON
= ALTER SAFEGUARD, TERMINAL-EXCLUSIVE-ACCESS ON
= ALTER SAFEGUARD, BLINDLOGON ON
= ALTER SAFEGUARD, PASSWORD-ENCRYPT ON
= ALTER SAFEGUARD, PASSWORD-MINIMUM-LENGTH 8
= ALTER SAFEGUARD, AUTHENTICATE-MAXIMUM-ATTEMPTS 3
= ALTER SAFEGUARD, AUTHENTICATE-FAIL-TIMEOUT 5 MIN
= ALTER SAFEGUARD, AUTHENTICATE-FAIL-FREEZE OFF
= ALTER SAFEGUARD, PASSWORD-HISTORY 10
= ALTER SAFEGUARD, NAMELOGON ON
= ALTER SAFEGUARD, CI-PROG $SYSTEM.SYSTEM.TACL
= ALTER SAFEGUARD, CI-LIB $SYSTEM.SYSTEM.<TACLMacro_lib>
= ALTER SAFEGUARD, CI-SWAP $<SwapVolume>
= ALTER SAFEGUARD, CI-CPU ANY
= ALTER SAFEGUARD, CI-PRI 150
= ALTER SAFEGUARD, CI-PARAM-TEXT <param_text>
```

SAFEGUARD: View Safeguard settings.

```
TACL> SAFECOM
= INFO SAFEGUARD, DETAIL
```

SECURITY: Prepare and alter security for system maintenance.

NOTE: Due to the nature of the work, while in maintenance mode the Tandem system may fall below the Class C2 level of security during the tool use.

```
TACL1>LOGON SUPER.SUPER (or SA USERID)
TACL2>FUP
=VOLUME $SYSTEM.SYSTEM
=SECURE (RCP, TMDS), "GOGO"
=SECURE (TMDSREP, TMDSREP2), "GOGO"
=VOLUME $SYSTEM.SYS<nn>
=SECURE (TMDSAUTO, TMDSLIB), "GOGO"
=EXIT
TACL3> OBEY $SYSTEM.<tmdssafeobey>.TMDSSAFE
```

- Log on to OSP/RMI or the system control panel via the function key. Turn over OSP/RMI or the control panel to Maintenance personnel.

- Monitor and manually log all functions performed by Maintenance personnel.

- When completed with maintenance, re-secure passwords.

SECURITY: Secure physical tape drive devices to prevent access during normal operations by the non-System Administration group and all Group Manager userids.

```
TACL>SAFECOM

= ADD DEVICE $TAPE1, OWNER 255,255, ACCESS 255,* (R,W)
= ALTER DEVICE $TAPE1, ACCESS *,255 (R,W)

= ADD DISKFILE (BACKUP, RESTORE, FUP), OWNER 255,255, access *,255 (R,E)
```

SECURITY: Secure software-debugging tools using FUP and SAFECOM to allow access by group managers.

FUP

```
TACL> FUP
=VOLUME $SYSTEM.SYS<nn>

=GIVE (DMON, IMON, INSPECT, INSPHELP), 255,255
=SECURE (DMON, IMON, INSPECT, INSPHELP), "OOOO"

=GIVE (INSPLOCL, INSPMSG), 255,255
=SECURE (INSPLOCL, INSPMSG), "OOOO"
```

SAFECOM

```
TACL>SAFECOM
= VOLUME $SYSTEM.SYS<nn>

= ADD DISKFILE (DMON, INSPECT, INSPHELP), OWNER 255,255
= ALTER DISKFILE (DMON, INSPECT, INSPHELP), ACCESS *,255 (R,E)
= FREEZE DISKFILE (DMON, INSPECT, INSPHELP)

= ADD DISKFILE (INSPLOCL, INSPMSG, IMON), OWNER 255,255
= ALTER DISKFILE (INSPLOCL, IMON, INSPMSG), ACCESS *,255 (R,E)
= FREEZE DISKFILE (INSPLOCL, IMON, INSPMSG)
```

SECURITY: Secure system configuration and other system administration tools to prevent unauthorized access.

```
TACL>LOGON SUPER.SUPER
TACL>FUP

=VOLUME $SYSTEM.SYS<nn>

=GIVE (COUP, DSC, DIVER, SWID, RELOAD, RCP), 255,255
=SECURE (COUP, DSC, DIVER, SWID, RELOAD, RCP), "OOOO"

=GIVE (CMILIB, CMPLIB, CMIHELP, CMT, CMTC, SCF, SCP), 255,255
=SECURE (CMILIB, CMPLIB, CMIHELP, CMT, CMTC, SCF, SCP), "OOGO"

=GIVE (SPOOL, CMI, CMP, ZELM, ZLOG, ZMOM, CUP), 255,255
=SECURE (SPOOL, CMI, CMP, ZELM, ZLOG, ZMOM, CUP), "OOGO"

=GIVE (DDNOBJ, DIAG3501, DIAG5000, DIAG6204), 255,255
=SECURE (DDNOBJ, DIAG3501, DIAG5000, DIAG6204), "OOOO"
```

```
=GIVE (FTPDDN, ODISCFA, ORSERV, INSTALL), 255,255
=SECURE (FTPDDN, ODISCFA, ORSERV, INSTALL), "OOOO"

=GIVE (OZEXP, SCPTC, SERVLAN, SERVSXLK, SYSGEN), 255,255
=SECURE (OZEXP, SCPTC, SERVLAN, SERVSXLK, SYSGEN), "OOOO"

=GIVE (COPYDUMP, TCPIP, MLMAN, MLSRV), 255,255
=SECURE (COPYDUMP, TCPIP, MLMAN, MLSRV), "OOOO"

=GIVE (DSXLKAM, FILCHECK, SERV6204, COVERCOM), 255,255
=SECURE (DSXLKAM, FILCHECK, SERV6204, COVERCOM), "OOOO"

=GIVE (CUPTRACE, SERVCSS, DIALFA, CHARON), 255,255
=SECURE (CUPTRACE, SERVCSS, DIALFA, CHARON),"OOOO"

=GIVE (CSSAM, CLXFA, MFCAM, SERVMFC, COMMAM), 255,255
=SECURE (CSSAM, CLXFA, MFCAM, SERVMFC, COMMAM), "OOOO"

=GIVE (OSL, TPIPTPRN, CPUFA, MDSFA, TMDSAUTO), 255,255
=SECURE (OSL, TPIPTPRN, CPUFA, MDSFA, TMDSAUTO), "OOOO"

=GIVE (TMDSLIB, APBFA, MEMFA, TAPEFA, DISCFA), 255,255
=SECURE (TMDSLIB, APBFA, MEMFA, TAPEFA, DISCFA), "OOOO"

=VOLUME $SYSTEM.SYSTEM

=GIVE (CPUSTAT, CPUCHG, MDSSTAT, MDSCHG, TMDS), 255,255
=SECURE (CPUSTAT, CPUCHG, MDSSTAT, MDSCHG, TMDS), "OOOO"

=GIVE (TMDSREP, TMDSREP2, IPBSTAT, GIOFDSPL), 255,255
=SECURE (TMDSREP, TMDSREP2, IPBSTAT, GIOFDSPL), "OOOO"

=GIVE (GIORELOC, TAPEEXER, TAPESTAT, TAPEPROB), 255,255
=SECURE (GIORELOC, TAPEEXER, TAPESTAT, TAPEPROB),"OOOO"

=GIVE (TAPETEST, TAPEVERF, DISCLOG, DISCSTAT), 255,255
=SECURE (TAPETEST, TAPEVERF, DISCLOG, DISCSTAT), "OOOO"

=GIVE (DISCLIST, DISCTEST, DISCUTIL, NETBATCH), 255,255
=SECURE (DISCLIST, DISCTEST, DISCUTIL, NETBATCH),"OOOO"

=GIVE (ODREV, ODSTAT, ODTEST, OFFSRV, DALSVR), 255,255
=SECURE (ODREV, ODSTAT, ODTEST, OFFSRV, DALSVR), "OOOO"

=GIVE (SQLCAT, SQLCOMP, SQLUTIL, VCSLIB, GOAWAY), 255,255
=SECURE (SQLCAT, SQLCOMP, SQLUTIL, VCSLIB, GOAWAY),"OOOO"
```

```
=GIVE $SYSTEM.ZGUARD.*, 255,255
=SECURE $SYSTEM.ZGUARD.*, "OOOO"

=GIVE $SYSTEM.SYS<nn>.DISCGEN, 255,255
=SECURE $SYSTEM.SYS<nn>.DISCGEN, "OOOO"

=GIVE $SYSTEM.A<SystemNumber>.*, 255,255
=SECURE $SYSTEM.A<SystemNumber>.*, "OOOO"
```

SECURITY: Secure system configuration tools to prevent access without SUPER.SUPER intervention.

```
TACL>SAFECOM
= VOLUME $SYSTEM.SYS<nn>

= ADD DISKFILE (COUP, DIVER, CMI, CMP, CMIHELP), OWNER 255,255
= ALTER DISKFILE (COUP, DIVER, CMI, CMP), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (COUP, DIVER, CMI, CMP, CMIHELP)

= ADD DISKFILE (CMIHELP, CMT, CMTC, DSC), OWNER 255,255
= ALTER DISKFILE (CMIHELP, CMT, CMTC, DSC), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (CMIHELP, CMT, CMTC, DSC)

= ADD DISKFILE (CMILIB, CMPLIB, RCP), OWNER 255,255
= ALTER DISKFILE (CMILIB, CMPLIB,RCP), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (CMILIB, CMPLIB, RCP)

= ADD DISKFILE (RELOAD, SPOOL, SWID), OWNER 255,255
= ALTER DISKFILE (RELOAD,SPOOL, SWID), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (RELOAD, SPOOL, SWID)

= ADD DISKFILE (DDNOBJ, DIAG6204, SCP), OWNER 255,255
= ALTER DISKFILE (DDNOBJ,DIAG6204,SCP),ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (DDNOBJ, DIAG6204, SCP)

= ADD DISKFILE (DIAG3501, DIAG5000), OWNER 255,255
= ALTER DISKFILE (DIAG3501, DIAG5000), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (DIAG3501, DIAG5000)

= ADD DISKFILE (FTPDDN, SCPTC), OWNER 255,255
= ALTER DISKFILE (FTPDDN, SCPTC), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (FTPDDN, SCPTC)

= ADD DISKFILE (ODISKFA, ORSERV, SCF), OWNER 255,255
= ALTER DISKFILE (ODISKFA, ORSERV, SCF), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (ODISKFA, ORSERV, SCF)

= ADD DISKFILE (OZEXP, MLMAN, SERVSXLK), OWNER 255,255
= ALTER DISKFILE (OZEXP, MLMAN, SERVSXLK),ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (OZEXP, MLMAN, SERVSXLK)

= ADD DISKFILE (SERVLAN, MLSRV, TCPIP), OWNER 255,255
= ALTER DISKFILE (SERVLAN, MLSRV, TCPIP), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (SERVLAN, MLSRV, TCPIP)

= ADD DISKFILE (CUP, SERVCSS, DSXLKAM), OWNER 255,255
= ALTER DISKFILE (CUP, SERVCSS, DSXLKAM), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (CUP, SERVCSS, DSXLKAM)

= ADD DISKFILE (FILCHECK, CSSAM, OSL), OWNER 255,255
= ALTER DISKFILE (FILCHECK, CSSAM, OSL), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (FILCHECK, CSSAM, OSL)

= ADD DISKFILE (CUPTRACE, COVERCOM), OWNER 255,255
= ALTER DISKFILE (CUPTRACE, COVERCOM), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (CUPTRACE, COVERCOM)

= ADD DISKFILE (SERV6204, CHARON), OWNER 255,255
= ALTER DISKFILE (SERV6204, CHARON), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (SERV6204, CHARON)

= ADD DISKFILE (ZELM, MFCAM, COPYDUMP), OWNER 255,255
= ALTER DISKFILE (ZELM, MFCAM, COPYDUMP), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (ZELM, MFCAM, COPYDUMP)

= ADD DISKFILE (CLXFA, DIALFA, COMMAM), OWNER 255,255
= ALTER DISKFILE (CLXFA, DIALFA, COMMAM), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (CLXFA, DIALFA, COMMAM)

= ADD DISKFILE (ZLOG, TPIPTPRN, CPUFA), OWNER 255,255
= ALTER DISKFILE (ZLOG, TPIPTPRN, CPUFA), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (ZLOG, TPIPTPRN, CPUFA)

= ADD DISKFILE (APBFA, MDSFA, SERVMFC), OWNER 255,255
= ALTER DISKFILE (APBFA, MDSFA, SERVMFC), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (APBFA, MDSFA, SERVMFC)

= ADD DISKFILE (MEMFA, TAPEFA, DISKFA), OWNER 255,255
= ALTER DISKFILE (MEMFA, TAPEFA, DISKFA),ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (MEMFA, TAPEFA, DISKFA)
= ADD DISKFILE (TMDASUTO, TMDSLIB), OWNER 255,255
= ALTER DISKFILE (TMDASUTO, TMDSLIB), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (TMDASUTO, TMDSLIB)

= ADD DISKFILE (ZMOM, MDSSTAT, MDSCHG), OWNER 255,255
= ALTER DISKFILE (ZMOM, MDSSTAT, MDSCHG), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (ZMOM, MDSSTAT, MDSCHG)

= VOLUME $SYSTEM.SYSTEM

= ADD DISKFILE (CPUSTAT, CPUCHG), OWNER 255,255
= ALTER DISKFILE (CPUSTAT, CPUCHG), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (CPUSTAT, CPUCHG)

= ADD DISKFILE (TMDSREP2, IPBSTAT), OWNER 255,255
= ALTER DISKFILE (TMDSREP2, IPBSTAT), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (TMDSREP2, IPBSTAT)

= ADD DISKFILE (TMDSREP, GIOFDSPL), OWNER 255,255
= ALTER DISKFILE (TMDSREP, GIOFDSPL), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (TMDSREP, GIOFDSPL)

= ADD DISKFILE (TAPESTAT, TAPEPROB), OWNER 255,255
= ALTER DISKFILE (TAPESTAT, TAPEPROB), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (TAPESTAT, TAPEPROB)

= ADD DISKFILE (GIORELOC, TAPEEXER), OWNER 255,255
= ALTER DISKFILE (GIORELOC, TAPEEXER), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (GIORELOC, TAPEEXER)

= ADD DISKFILE (TAPETEST, TAPEVERF), OWNER 255,255
= ALTER DISKFILE (TAPETEST, TAPEVERF), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (TAPETEST, TAPEVERF)

= ADD DISKFILE (DISKSTAT, DISKLOG), OWNER 255,255
= ALTER DISKFILE (DISKSTAT, DISKLOG), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (DISKSTAT, DISKLOG)

= ADD DISKFILE (DISKTEST, DISKUTIL), OWNER 255,255
= ALTER DISKFILE (DISKTEST, DISKUTIL), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (DISKTEST, DISKUTIL)

= ADD DISKFILE (OFFSRV, ODTEST, ODREV), OWNER 255,255
= ALTER DISKFILE (OFFSRV, ODTEST, ODREV), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (OFFSRV, ODTEST, ODREV)
= ADD DISKFILE (ODSTAT, SQLUTIL), OWNER 255,255
= ALTER DISKFILE (ODSTAT, SQLUTIL), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (ODSTAT, SQLUTIL)

= ADD DISKFILE (DISKLIST, NETBATCH), OWNER 255,255
= ALTER DISKFILE (DISKLIST, NETBATCH), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (DISKLIST, NETBATCH)

= ADD DISKFILE (SQLCAT, SQLCOMP), OWNER 255,255
= ALTER DISKFILE (SQLCAT, SQLCOMP), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (SQLCAT, SQLCOMP)

= ADD DISKFILE (TMDS, DALSVR), OWNER 255,255
= ALTER DISKFILE (TMDS, DALSVR), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (TMDS, DALSVR)

= ADD DISKFILE (VCSLIB, GOAWAY), OWNER 255,255
= ALTER DISKFILE (VCSLIB, GOAWAY), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (VCSLIB, GOAWAY)

= VOLUME $SYSTEM.ZGUARD

= ADD DISKFILE (SYSGENR, SYSGEN, INSTALL), OWNER 255,255
= ALTER DISKFILE (SYSGENR, SYSGEN, INSTALL), ACCESS 255,* (R,W,E)
= FREEZE DISKFILE (SYSGENR, SYSGEN, INSTALL)

= ADD DISKFILE $SYSTEM.SYS<nn>.DISKGEN, OWNER 255,255
= ALTER DISKFILE $SYSTEM.SYS<nn>.DISKGEN, ACCESS 255,* (R,W,E)
= FREEZE DISKFILE $SYSTEM.SYS<nn>.DISKGEN

= ADD DISKFILE $SYSTEM.A<SYSTEMNUM>.CUSTFILE, OWNER 255,255
= ALTER DISKFILE $SYSTEM.A<SYSTEMNUM>.CUSTFILE, ACCESS & 255,255
    (R,W,E,O)
= FREEZE DISKFILE $SYSTEM.A<SYSTEMNUM>.CUSTFILE
```

SECURITY: Secure the TM/MP transaction data audit to prevent unauthorized access during normal operations and without SUPER.SUPER intervention.

SAFECOM

```
TACL>SAFECOM
= ADD DISKFILE $SYSTEM.TMF.*, OWNER 255,255
= ALTER DISKFILE $SYSTEM.TMF.*, ACCESS 255,* (R,W,P)
= ALTER DISKFILE $SYSTEM.TMF.*, ACCESS *,* (R)
```

TACL

```
TACL1>LOGON SUPER.SUPER
TACL2>FUP GIVE $SYSTEM.TMF.*, 255,255
TACL3>FUP SECURE $SYSTEM.TMF.*, "OOOO"
```

SECURITY: Secure the userid file to prevent unauthorized access during normal operations without SUPER.SUPER intervention.

SAFECOM

```
TACL>SAFECOM
= VOLUME $SYSTEM.SYSTEM
= ADD DISKFILE (USERID, USERIDAK), OWNER 255,255
```

TACL

```
TACL>VOLUME $SYSTEM.SYSTEM
TACL>FUP GIVE (USERID, USERIDAK), 255,255
TACL>FUP SECURE (USERID, USERIDAK), "OOOO"
```

SECURITY: Third-party monitoring or security software packages implementation considerations.

There is a 3rd-party, PC-based software product called TIC. It reads the standard Tandem EMS logfiles, EMS distributors (EMSDIST) messages, filters event messages based on specific criteria, and displays a graphical representation of device and application status and warning messages on a PC. This could be used for network management or monitoring, and potentially it can also notify support personnel of problems.

SQL: Address SQL database table views separation.

These could be protected views where controls are put in the element levels of the rows and columns to prevent access to specific information if it meets a specific criteria (i.e., > 100,000).

Server 1 uses partial view A.
Server 2 uses protected view B.
Server 3 uses view C (full view).
User group A only has access to server 1 or 2 protected views.

SCREEN NAME	*RELATED SERVER*	*TABLE NAME*	*VIEW NAME*	*RULES*
APMENU01	APMENUS	Security Matrix	PA-View-Only	See only AP data
APEMP01	APEMP-Update	AP-EMP-Data	AP-EMP-Full	All EPEmp data
APEMP02	APEMP-Inquire	AP-EMP-Data	AP-EMP-Inq-Only	Selected AP-Emp

SQL: Implement SQL catalog and database security (R,W,E,P,O).

```
SQLCI ALTER CATALOG $Volume.Subvol SECURITY "GOGO", OWNER USER
GROUPID,USERID
```

SUPER-GROUP: Implement the super-group Kernel userids (TACL and BOSS).

Set default SUPER.SUPER password and defaults; create super-group userids, set default passwords, and set user default volumes, subvolumes, and security settings:

```
TACL
TACL1 > LOGON SUPER.SUPER
TACL2 > PASSWORD<password>
TACL3 > DEFAULT $Uservol.U255255,"OOOO"
```

```
TACL4 > ADDUSER SUPER.SO1, 255,001
TACL5 > ADDUSER SUPER.SO2, 255,002
TACL6 > ADDUSER SUPER.SO3, 255,003
TACL7 > ADDUSER SUPER.SO4, 255,004

TACL8 > LOGON to SUPER.SO1,
TACL9> PASSWORD <Password>
TACL10> DEFAULT $Uservol.U255001,"OOOO"

TACL11> LOGON to SUPER.SO2,
TACL12> PASSWORD <Password>
TACL13> DEFAULT $Uservol.U255002,"OOOO"

TACL14> LOGON to SUPER.SO3,
TACL15> PASSWORD <Password>
TACL16> DEFAULT $Uservol.U255003,"OOOO"

TACL17> LOGON to SUPER.SO4,
TACL18> PASSWORD <Password>
TACL19> DEFAULT $Uservol.U255004,"OOOO"
```

BOSS

See *Section C.2, How to Add Users/Applications* of the *BOSS Block-mode Operating System Services User's Guide, Version 4.0K.*

TACL: Implement the password program configuration options (edit mask) restrictions to improve security for command-level access (TACL and COMINT).

```
TACL> RENAME
$SYSTEM.SYS<nn>,PASSWORD,$SYSTEM.OSYS0.PASSWORD
TACL> BIND
@ ADD CODE $SYSTEM.OSYS<nn>.PASSWORD
@ ADD DATA $SYSTEM.OSYS<nn>.PASSWORD

@ MODIFY DATA ENCRYPTPASSWORD HEX, 1
@ MODIFY DATA BLINDPASSWORD HEX, 1
@ MODIFY DATA MINPASSWORDLEN HEX, 8
@ MODIFY DATA PROMPTPASSWORD HEX, 1
@ BUILD $SYSTEM.SYS<nn>.PASSWORD
@ EXIT
```

TACL: Implement the TACL restrictions for command-level access.

The following nine TACL parameters will be set to ensure access restrictions are enforced for all system command-level access using TACL:

-	*AUTOLOGOFFDELAY*	*ON (15 minutes)*
-	*CMONREQUIRED*	*OFF*
-	*CMONTIMEOUT*	*(30 seconds)*
-	*BLINDLOGON*	*ON*
-	*NAMELOGON*	*ON*
-	*NOCHANGEUSER*	*OFF*
-	*REMOTECMONREQUIRED*	*OFF*
-	*REMOTECMONTIMEOUT*	*(30 seconds)*
-	*REMOTESUPERID*	*OFF*

NOTE: The manual that addresses these TACL options suggests they are modified only by the Tandem Support Analyst, and have to be reset each time a SYSGEN is performed.

TACL: View the current password restrictions for command-level access.

The password program can provide the following strong password restrictions on the Kernel userids as described in *Section 4.1.4, Guidelines for Strong Passwords and User Locking*. The IAO will ensure the following restrictions are established for the copy of the password program not used by BOSS:

```
TACL> LOGON SUPER.SUPER
TACL> VOLUME $SYSTEM.BOSS
TACL> FUP DUP SYS<nn>.PASSWORD, BOSS.*, SAVEALL
TACL> BIND
@ DUMP DATA ENCRYPTPASSWORD * FROM $SYSTEM.SYS<nn>.PASSWORD
@ DUMP DATA BLINDPASSWORD      * FROM $SYSTEM.SYS<nn>.PASSWORD
@ DUMP DATA MINPASSWORDLEN    * FROM $SYSTEM.SYS<nn>.PASSWORD
@ DUMP DATA PROMPTPASSWORD    * FROM $SYSTEM.SYS<nn>.PASSWORD
@ DUMP DATA PROMPTPASSWORD * FROM $SYSTEM.BOSS.PASSWORD
@ EXIT
```

TACL: View the current TACL restrictions for command-level access.

Use the TACL command #GETCONFIGURATION to display them.

```
TACL1> #GETCONFIGURATION/ AUTOLOGOFFDELAY /
TACL2> #GETCONFIGURATION/ CMONREQUIRED /
TACL3> #GETCONFIGURATION/ CMONTIMEOUT /
TACL4> #GETCONFIGURATION/ BLINDLOGON /
TACL5> #GETCONFIGURATION/ NAMELOGON /
TACL6> #GETCONFIGURATION/ NOCHANGEUSER /
TACL7> #GETCONFIGURATION/ REMOTECMONREQUIRED /
TACL8> #GETCONFIGURATION/ REMOTECMONTIMEOUT /
TACL9> #GETCONFIGURATION/ REMOTESUPERID /
```

APPENDIX E. "HOW TO" GUIDE FOR BOSS

Installation and Configuration

A. INTRODUCTION

The BOSS product is used to provide secure audited access control for application-level users and for most system-level users. This appendix explains how to implement the BOSS COTS product in conjunction with Kernel and application userids. The system-level access control issues of full Kernel command-level access discussed in *Section 4.2.2.2, Full Kernel Command-level Access*, and *Section 4.2.2.4, Kernel Limited Command-level Access*, are intended to be addressed using BOSS menus and submenus. The following sections provide details for the corresponding items listed in S*ection C, Installation and Configuration Details*, of this appendix.

B. INSTALLATION AND CONFIGURATION SUMMARY

To implement the BOSS COTS product, follow the process described below and detailed in the instructions listed in *Section C, Installation and Configuration Details*, of this appendix.

1. Install the BOSS software.

2. Create, configure, secure, and start the BOSS Pathway system and database.

3. Establish and configure the BOSS global parameters.

4. Define, set up, and properly secure all entities to be controlled through BOSS. The application-level users, System Administration users, Operations users, the terminals used to access the system, the remote nodes to be accessed, the initial logon screens, security disclaimers, the applications to be accessed, required assigns, required parameters, BOSS utilities, and system utilities all need to be defined in BOSS. After all the related resources have been defined to BOSS, establish appropriate linkages in BOSS.

   Link terminals to title records (initial logon screen).

   a. Define logical application userids as required.

   b. Define Kernel userids for SAs and system operators as required.

   c. Establish access records for staff that require Kernel utilities and BOSS utilities including SAs and system operators.

   d. Define the units of work (applications, functions, system utilities, and commands) that are available through BOSS.

e. Define assigns and parameters as needed by applications and link them appropriately.

f. Define profile records and associated functions and flags as needed by applications and link them appropriately.

g. Define the Pathway systems external to BOSS for linkage and access to them.

h. Establish groups for users based on access needs and group applications into menus or submenus. Then link the user groups and application groups to the menu or submenus.

i. Establish a group(s) for System Administration and system Operations users and define the functions they need and are authorized for into separate groups with separate menus or submenus.

j. For users that have authorized access to Command Interpreter utilities and audited utility sub-commands, establish the access in BOSS as needed.

k. Link the grouping of user domains and applications to be accessed.

5. Secure default BOSS userids that were delivered with the COTS software package. Change the password for the BOSS logical user BOSS.MAINT.

C. INSTALLATION AND CONFIGURATION DETAILS

1. Install BOSS as directed by the vendor.

2. Configure the BOSS Pathway system.

a. Migrate relevant existing SAS security information into the BOSS database.

b. Secure the entire BOSS software, database, and configuration files to the appropriate SA userid.

c. Start the BOSS Pathway system.

3. Define the BOSS global defaults set in the BOSSENV file.

   a. Use the **BOSSMAINT Available Program Menu** screen to access the next screen. Then use the **BOSS Configuration Subsystem Environment File Maintenance** screen to define the appropriate BOSS global Environment Key record (for the BOSS Pathway system) restrictions with the related password restrictions (as discussed in *Section 4.1.4, Guidelines for Strong Passwords and Userid Locking*). Apply the following parameters:

      (1) Set the **Safeguard Installed** value to **N** if this site is not using Safeguard to aid in system security, and **Y** if Safeguard is used.

      (2) Set the **Advanced Auditing** value to **Y**.

      (3) Set the **Password Generations** value to 10.

      (4) Set the **Min Length of Password** value to 8.

      (5) Set the **Min Alpha Characters** value to **1**.

      (6) Set the **Min Numeric Characters** value to **1**.

      (7) Set the **Max Occurrences** value to **2**.

      (8) Set the **Max Logon Attempts** value to **3** to cause userid access through BOSS to freeze after three invalid logon attempts.

      (9) Set the **Advanced Auditing Info Default Action** value to **D** (Deny) or **G** (Grant). (**D** is recommended.)

      (10) Set the **Advanced Auditing Info Default Mode** value to **N** (Normal) or **W** (Warning). (**N** is required.)

      Define, set up, and link the elements to be controlled by BOSS.

b. Link terminals to title records (initial logon screen).

Use the **BOSSMAINT Available Program Menu** screen to access the next screen. Then use the **BOSS Configuration Subsystem BOSS Terminal File Maintenance** screen to access the next screen, and use the **BOSS Configuration Subsystem BOSS Title File Maintenance** screen to do the following:

(1) Define the appropriate **Title Record** (for the initial logon screens) with the appropriate security disclaimer for the system as discussed in *Section 4.1.1, Warning Legal Notice of Display Devices*.

(2) Set the **Show Copyright Notice** value to **Y**.

(3) Set the terminal **Screen Timeout** value to **900. (900 Seconds = 15 Minutes)**

Use the **BOSSMAINT Available Program** menu to access the next screen. Then use the **BOSS Configuration Subsystem BOSS Terminal File Maintenance** screen to do the following:

(1) Establish in the BOSS **Logical Term Name** field a default terminal record to associate to the default **Title Key** record and the default language. To support user access other than the default terminal record, add specific Pathway **Logical Term Name** terminal records as necessary. For example, a user that requires another language other than the default (English) on the terminal. Exclude from this list of terminals defined to BOSS the two terminals that require non-BOSS TACL access that are in the secured area.

(2) Set the **Title Key** value to the appropriate **Title Name** value from the corresponding **Title Record**. This links (assigns) the appropriate **Title Record** (initial logon screens) with the appropriate terminals on the system.

(3) Set the **Language** value to **0**.

c. Define application userids to BOSS.

Use the **BOSSMAINT Available Program** menu to access the next screen. Then use the **BOSS Configuration Subsystem User File Maintenance** screen to do the following:

(1) Define the user information to BOSS for the application users. Enter the appropriate unique information (groupname and username and corresponding groupnumber and usernumber), and related password restrictions as discussed in *Section 4.1.4, Guidelines for Strong Passwords and Userid Locking*. Take care to assign only one groupnumber to one corresponding groupname, and within a group to assign only one usernumber to one corresponding username.

(2) Set the **Days before password MUST Change** value to **90**.

(3) Set the **Days before password MAY Change** value to **1**.

(4) Set the **Max Sessions** value to **1** for all application users.

(5) Set the **User Timeout** value to **900** for all application users.

(6) Set the **NSK User** value to **N** for logical users. Set the **NSK User** value to **Y** for **NSK** users.

NOTE: For logical users, do not put any value in the group ID or userid fields.

(7) Set the **Disable User** value to **N**.

(8) Set the **Global Password** value to **N**. Global passwords are not allowed for any users because this feature reduces the security level of the entire network and introduces a potential vulnerability.

(9) Set the **Enterprise Password** value to **N**.

(10) Set the **Password Only** value to **N**.

d. Define Kernel userids for the SAs and system operators in BOSS. Take care to assign only one groupnumber to one corresponding groupname, and within a group to assign only one usernumber to one corresponding username.

Use the **BOSSMAINT Available Program** menu to access the next screen. Then use the **BOSS Configuration Subsystem User File Maintenance** screen to do the following:

(1) Define the user information to BOSS for the SAs and system operators. Link these IDs to Kernel userids, and establish the related password restrictions as discussed in *Section 4.1.4, Guidelines for Strong Passwords and Userid Locking*. Enter the appropriate unique information (logical groupname and corresponding groupnumber, username and corresponding usernumber).

(2) Set the **Days before password MUST Change** value to **90**.

(3) Set the **Days before password MAY Change** value to **1**.

(4) Set the **Max Sessions** value to from **1** to not more than **4** for all SAs and system operator users.

(5) Set the **User Timeout** value to **900** for all logical application users.

(6) Set the **NSK User** value to **Y** unless this user has not been authorized access to Kernel tools.

(7) Set the **Disable User** value to **N**.

(8) Set the **Global Password** value to **N**. Global passwords are not allowed for any users because this feature reduces the security level of the entire network and introduces a potential vulnerability. Global passwords must not be used for any System Administrator userids.

(9) Set the **Enterprise Password** value to **N**.

(10) Set the **Password Only** value to **N**, and do one of the following:

From the **Available Program Menu** screen, select the **BOSSMAINT BOSS Maintenance** screen to access the **BOSSMAINT Available Program Menu** screen. Then select the **BOSS_BOSSID BOSS User File Maintenance** screen to access the **BOSS Configuration Subsystem User File Maintenance** screen to access the F1 **User Directory** option to access the **BOSS Configuration Subsystem BOSS User Directory File Maintenance** screen.

(or)

From the **Available Program Menu** screen, select the **BOSS User Directory Services** screen to access the **BOSS Utilities Directory Services** screen.

(and)

Define the user information in BOSS used for the password verification on the **BOSS Utilities Directory File Maintenance** screen.

e. Use the **BOSSMAINT Available Program Menu** to access the next screen. Then use the **BOSS Configuration Subsystem User File Maintenance** screen. Then use F3 to access the **BOSS Configuration Subsystem User/Node File Maintenance** screen to define remote access for those users with the requirement. It is accomplished by doing the following:

(1) Identify the users that require multi-node access, applications that require remote node access, and to which nodes each user requires access.

(2) Create a record for each user with remote node access requirements. A separate BOSS node file record must be created to link each remote node to be accessed with each corresponding user that has the remote access requirement. Add relevant information (groupname, username, and nodename of the remote site where access is required) to BOSS in the user/node file maintenance screen.

(3) The **Global Password** option must be set to **N** for all users. Global passwords are not allowed for any users because this feature reduces the security level of the entire network and introduces a potential vulnerability. Global passwords must not be used for any System Administrator userids.

f. Define the units of work (applications, functions, utilities, and commands).

Use the **BOSS Configuration Subsystem Application Information File Maintenance** screen to do the following:

(1) Define the units of work (Gateway, applications, requestor utility, and BOSS services).

(a) Set the **Program ID** field to a unique name that will be used on the available menu screens within BOSS to refer to this application or function.

(b) Set the **Menu Description** field to the descriptive name that will appear on the available menu screens within BOSS when referring to this application or function.

(c) Set the **Object** field to the actual file name of the program, requestor name, or function to be executed when this menu item is selected.

(d) Set the **Input File Name** to the input location desired if other than the user's terminal.

(e) Set the **Output File Name** to the output location desired if other than the user's terminal.

(f) Set the **Command Line** field to the startup command stream to be passed to this process when it is executed.

(g) Set the **Type of Object**, **Run Time Priority**, **CPU to Use**, **Startup Volume**, and **Startup Subvol** fields to the appropriate values based on the variables listed in the BOSS User's Guide provided by the vendor.

(h) If the application/program is to run under the current ID, the **Run As** field will be blank. Otherwise, the **Run As** field will contact the groupnumber and usernumber the application/program is to run under.

NOTE: Page down to access the items in (**i**) below.

(i) Set the **Run High Pin**, **Run Nowait**, **Prompt After Running**, **Record Disabled**, **Requester Linkage**, **Does Record have Assigns**, and **Does Record have Params** fields to the appropriate values based on the variables listed in the BOSS User's Guide provided by the vendor**.**

(2) Define the applications to be accessed through BOSS.

(a) The **Run in Debug** field must always be set to the value of **N**. The only allowed exception is while specific authorized problem resolution is occurring. During this problem resolution time, the value of this field may be temporarily altered to **Y**.

(b) The use of advanced auditing must be enabled to allow auditing of user activity at the level of this function. To accomplish this, the **Audit This Record** field value must be set to **Y**. It may be set to **N** for some applications at the discretion of the IAO.

(3) Define the system utilities to be used by limited users and operations users with BOSS menus.

The use of advanced auditing must be enabled to allow auditing of user activity at the level of this function. To accomplish this, the **Audit This Record** field value must be set to **Y**. The value of this field must always be set to **Y** for all command-level and utility access.

(4) Define the **CLFPROG** (CLF **Applinfo** record) and other BOSS utilities as required for BOSS and documented in the vendor manual. These are used for advanced auditing features of BOSS.

(a) This function in BOSS performs the advanced auditing on behalf of other functions. Therefore, this function should not be executed directly from a user and access to the CLFPROG record does not need to be audited. The **Audit This Record** field value should be set to **N**.

(b) The value of the **Run As** field must be blank.

g. Define assigns and parameters as needed by units of work (applications and functions).

Use the **BOSS Configuration Subsystem Applinfo/Assign File Maintenance** screen to do the following:

(1) Create and verify the assigns for the CLF **Applinfo** record and all other applications that require assigns.

(a) Set the **Applinfo Key** field to match the name of the Application Information File record **Program ID** for which this assign will be used within BOSS.

(b) Set the **Assign Key** field to the unique name of the assign for the Application Information File record **Program ID** to which this assign applies.

(c) Next select the F1 **Assign Detail** function key from this screen, and define the actual file name to be assigned using each assign key established in the previous step.

Use the **BOSS Configuration Subsystem Applinfo/Param File Maintenance** screen to do the following:

(2) Create and verify the parameters for the CLF **Applinfo** record and all other applications that require parameters.

(a) Set the **Applinfo Key** field to match the name of the Application Information File record **Program ID** for which this parameter will be used within BOSS.

(b) Set the **Parameter Key** field to the unique name of the parameter for the Application Information File record **Program ID** to which this parameter applies.

(c) Next select the F1 **Parameter Detail** function key from this screen, and define the actual default value of the parameters to be passed using each parameter key established in the previous step.

h. Defining the profile records for the applications in BOSS.

Use the **BOSS Advanced Application Service/Application Profile Maintenance** screen to define each profile for an application and link a profile to an application. The intent of a BOSS profile is to provide a mechanism to allow the grouping of functions a user can perform. The intent of a BOSS function is to allow a mechanism to identify a specific application function or screen within the application with a code for access control and auditing.

(1) Define in BOSS the appropriate profile records for each application.

(a) Set the **Profile Key: Appl Id** field to match the name of the Application Information File record **Program ID** to which this profile will be associated within BOSS.

(b) Set the **Profile Key: Profile** field to the unique name of the profile for the application to which this profile applies.

(2) Define in BOSS the function and flags related to each profile for each application.

(a) Set the **Profile Key: Function** field to the appropriate value for the functions of this profile authorized for users to perform within the application.

(b) Set the **Detail: Flags** field to appropriate flag names that will be passed values by the user when using this application and the related profile. For Navy applications, enter **Y** in this field to indicate an **activity code** is required by this application, or leave blank if the application does not require an **activity code**.

(or)

Use the **BOSS Configuration Subsystem Application Profile Definition** screen to define each profile for an application and link or assign a profile to an application.

(3) Define in BOSS the appropriate profile records for each application and the application to profile link for each profile.

(a) Set the **Profile Key: Appl Id** field to match the name of the Application Information File record **Program ID** to which this profile will be associated within BOSS.

(b) Set the **Profile Key: Profile** field to the unique name identifying this profile to which the application applies.

(c) Set the **Detail: Description** field to an appropriate description regarding the use of this profile and what functions this profile will authorize users to perform within this application.

(4) Define in BOSS the **SCOPE** function related to each profile for each application.

(5) Define in BOSS the flags related to each profile for each application.

(a) Set the **Detail Flags** field to appropriate flag names that will be passed values by the user when using this application and the related profile. For Navy applications, enter **Y** in this field to indicate an **activity code** is required by this application, or leave blank if the application does not require an **activity code**.

(b) Set the **Disabled** flag to **N** to enable the use of this application profile record.

Use the **BOSS Configuration Subsystem Function File Maintenance** screen to define each function associated with this profile record.

(6) Define in BOSS the appropriate function file records associated with these profile records for each application.

(a) Set the **Profile Key: Appl Id** to the appropriate application or function that will be associated with this function file record.

(b) Set the **Profile-Key: Profile** to the appropriate function name associated with this function so it can be linked to a profile.

(c) Set the **Detail: Description** to an appropriate description regarding the use of this function within the application profile.

(d) Set the **Detail: Scope** to an appropriate **Program ID** value as defined in the corresponding Application Information File record for this application, or leave blank if the function does not require a **Program ID**.

(e) Set the **Detail: Flags** to appropriate flag names that will be passed values by the user when using this application and the related profile. (This field is normally left blank.)

(f) Set the **Detail: Disabled** flag to **N** to enable use of this function file record.

i. Define the user to application profile links in BOSS. The information in this section is subject to change based on on-going review.

Use the **BOSS Configuration Subsystem User/Application Profile Maintenance** screen to define each link associating user access with profile records.

Define in BOSS the user authorization to access the associated application profile records for each application.

(1) Set the **BOSS ID Group** field to the appropriate groupname for the user that will be authorized access to this application profile.

(2) Set the **BOSS ID User** field to the appropriate userid for the user that will be authorized access to this application profile.

(3) Set the **Application Info Name** field to match the name of the Application Information File record **Program ID** that this profile is associated to and this user is authorized to access from within BOSS.

(4) Set the **Application Info Profile** field to match the name of the appropriate profile associated with this application that this user is authorized to access from within BOSS.

j. Define the external application Pathway links to BOSS.

Use the **BOSS Configuration Subsystem PathLink File Maintenance** screen to define the Pathway links for external Pathways (non-BOSS).

(1) Set the **PathInfo Key** field to the appropriate name for the external Pathway (this must match the application information file record defined to BOSS for this Pathway link) the users will be authorized to access.

(2) Set the **Target Node Name** field to the appropriate remote node name for authorized Pathway systems that resides on other remote nodes. If this Pathway executes on the same node as this BOSS system, leave this field blank.

(3) Set the **Target Pathway Name** field to match the name of the Pathway monitor that is executing for this Pathway system.

(4) Set the **6530 Requester Name** and the **3270 Requester Name** fields to the appropriate values to ensure the requester screen being accessed in the Pathway system being linked to will enforce all relevant security as defined in the *Tandem STIG*.

(5) Set the **Pass Security Information** field to **N** if the Pathway system being accessed is on a different node. This value may be set to **Y** if the Pathway system being linked to is on the same node as the BOSS.

(6) Set the **Custom Services** field to **N**.

(7) Set the **Leave Terminal Configured** field to **N**.

(8) Set all other related fields as appropriate to correspond with the Pathway system link.

k. Define the application menu and submenus to BOSS.

Use the **BOSS Configuration Subsystem MenuInfo File Maintenance** screen to define the available applications for each user and group of users.

Define the menu groups and submenus for each user and group of users.

(1) Set the **Group Name** field to an appropriate groupname for the user that will be authorized access to this application or function.

(2) Set the **User Name** field to an appropriate username for the user that will be authorized access to this application or function.

(3) Set the **List** field to a sequence number that will be used to determine the order in which the menu choices will be offered to the user.

(4) Set the unnamed field below the username field to match the name of the Application Information File record **Program ID** that this user is authorized to access from within BOSS.

l. Define the System Administration menu and submenus.

Use the **BOSS Configuration Subsystem Application Information File Maintenance** screen to define the available applications. After defining the applications and menus, use the **BOSS Configuration Subsystem MenuInfo File Maintenance** screen to associate the required available applications with each user or group of users.

(1) Define the menu groups and submenus for each SA and SA group. Include access to the following BOSS required objects as menu items:

Menu (Program ID)	**Object Name**
BOSSMAINT	
APPL-INFO	APPLINFO-MAINT
APPL-PROFILE-DETAIL	APPL-PROFILE-DETAIL
APPL-PROFILE-MAINT	APPL-PROFILE-MAINT
BOSSENV	BOSSENV-MAINT
BOSSID	BOSSID-MAINT4
FLAGS-FILE	FLAGS-MAINT
FUNCTIONS-FILE	FUNCTIONS-MAINT
MENU-MAINT	MENUINFO-MAINT2
PROFILE-DEF	APPL-PROFILE-DETAIL-MAINT
PROFILE-DETAILS	APPL-PROFILE-MAINT
TERM	BOSSTERM
DIR (DIRECTORY SERVICES)	USER-DIRECTORY2
USER-PROFILE	USER-APPLICATION-PROFILE
USERNODE	USER-NODE-MAINT4
CI-PROFILE	CLFPROFILE-MAINT
PASSWORD (UTILITY)	PASSWORD-TAN
DOMAINMAINT	
DOMAIN	DOMAIN-MAINT
DOMAIN-USER	USER-DOMAIN-MAINT
DOMAIN-APPLID	APPLID-DOMAIN-MAINT
DOMAIN-PROFILE	PROFILE-DOMAIN-MAINT
SCOPEMAINT	
SCOPE-DEFINITIONS	SCOPE-DEFINITIONS-MAINT
SCOPE-DETAILS	SCOPE-DETAILS-MAINT
SCOPE- PARTICIPANT-ID-MAINT	PARTICIPANT-ID-MAINT
SCOPE-FI-MAINT	FI-MAINT

(2) After defining the SA menus and submenus, disable access to the following BOSS objects and the respective menu names:

Menu (Program ID)	**Object Name**
SCOPEMAINT	
USERNODE	USER-NODE-MAINT4
SCOPE-DEFINITIONS	SCOPE-MAINT
SCOPE-DETAILS	SCOPE-DETAIL-MAINT
SCOPE-PARTICIPANT-ID-MAINT	PARTICIPANT-ID-MAINT
SCOPE-FI-MAINT	FI-MAINT

m. Establish the BOSS Command Interpreter and Kernel utility-level interface information.

Use the **BOSS Configuration Subsystem CI Profile File Maintenance** screen to define the BOSS-monitored system utility access for each system utility that will be authorized access through BOSS. These utilities will generally be for the Help Desk users, system operators, and other command-level user access. (Refer to *Section 4.2.2, System-level Access Control*, for specific policy guidance.)

Create a BOSS CI Global defaults record in the CI Profile file for each utility that will be granted access. To create each record, do the following:

(1) Set the **Default CI Mode** value to **G** (grant access).

(2) Set the **Log ALL CI Activity** value to **Y**.

***NOTE*:** Block-Mode flow will cause an abundance of audit data.

(3) Set the **CI Running Mode** value to **N** (normal access).

(4) Set the inactivity **CI Timeout Value** to **15** minutes.

Use the **BOSS Configuration Subsystem CI Command File Maintenance** screen to define the system utility commands that are allowed through BOSS. This provides command-level DAC for the system utilities defined in the previous step. Each specific system utility for which users require command-level access must be controlled and defined to BOSS with this screen. (Refer to *Section 4.2.2, System-level Access Control*, for policy guidance.)

Create a BOSS CI Command defaults record in the CI Command file for each utility command for which users will have authorization. To create each record, do the following:

(1) Set the **Name of Command Interpreter** value to the name of the **Applinfo** record for the system utility to be executed.

(2) Set the **CI Command** value to the actual name of the command for the system utility to which access is required.

(3) Set the **Default Command Processing Approval Setting** value to **D.** (This will deny access to all users unless specifically granted at the next level.)

(4) Set the **Command Running Mode** value to **N** (normal access).

(5) Set the **Log This Command** value to **Y**. (Generate a log record each time this record is accessed.)

(6) Set the **Check the User for This Command** value to **Y**. (This will force BOSS to check the user records for deny/grant access.)

Use the **BOSS Configuration Subsystem User Command File Maintenance** screen to define the BOSS-allowed user access for the system utility commands. Each specific system utility command that requires user-level access control will need a record defined for each user or group of users of the utility command that will be authorized access. (Refer to *Section 4.2.2, System-level Access Control,* for policy guidance.)

Create a BOSS CI Command user defaults record in the CI Command user file for each user of each utility command that will be granted access. To create each record, do the following:

(1) Set the **Name of Command Interpreter** value to the name of the **Applinfo** record for the system utility to be executed.

(2) Set the **Command** value to the actual name of the command for the system utility to which access is required.

(3) Set the **User ID** value to the groupname and username of the user to which access for this command is allowed.

(4) Set the **Run As ID** value (groupname) to "*****" (this prevents non-NSK groups from executing this command).

(5) Set the **Run As ID** value (userid) to "*****" (this prevents non-NSK users from executing this command).

(6) Set the **Command Processing Setting** value to **G** (grant).

(7) Set the **Command Mode** value to **N** (normal access).

(8) Set the **Log this Command** value to **Y**.

n. Define the domains and link the appropriate users to them. Before defining the domains, review all records for the domains and the users that are currently members. Delete any inappropriate entries. Insert records with the appropriate information for any missing domains and domain user members. The following information will be needed for each domain and user that will be added as a member of a domain.

Domains are used to group the users by job function. Use the **BOSS Advanced Application Services DomainMaint Available Program Menu [F1]** to access the next screen, and use the **BOSS Advanced Application Services Domain File Definition** screen to do the following:

(1) Define in BOSS the name of the domain. Set the **Domain Name** field to a meaningful name for this domain.

(2) Set the **Description** field to a meaningful description for this domain name.

(3) Set the **Disable Flag** value to **N** (enable access for this domain).

Use the **BOSS Configuration Subsystem Domain Applid File Maintenance** screen **[F2]** to define the links between a domain and the applications or functions available to the users of the domain by doing the following.

Create the domain **Applid** file records for each application to be available in this domain.

(1) Set the **Domain Name** field to the name of the domain to update.

(2) Set the **Applid** field to the name of the function or application that needs to be made available as a function in this domain. The **Applid** name identified in this screen must be the same as the **Program ID** defined in the Application Information file record for this function or application.

Use the **BOSS Advanced Application Services Domain/Profile File Maintenance** screen **[F3]** to define the application profiles that will be available for the application in this domain by doing the following.

Create the domain/profile file records and link the application-associated profiles to the domains.

(1) Set the **Domain Name** field to the name of the domain to update.

(2) Set the **Profile Key: Applid** field to the name of the function or application that needs to be associated with this profile. This provides the authorized access link to this domain. The **Applid** name identified in this screen must be the same as the **Program ID** defined in the Application Information file record for this function or application.

(3) Set the **Profile Key: Profile** field to the appropriate associated application profile name.

(4) Access the **BOSS Configuration Subsystem Application Profile Definition** screen by selecting the **Profile Detail** function key **[F2]** from this screen.

  (a) Set the **Profile Key: Applid** field to the name of this function or application that needs to be associated with this profile. This provides the authorized access link to this domain. The **Applid** name identified in this screen must be the same as the **Program ID** defined in the Application Information file record for this function or application.

  (b) Set the **Profile Key: Profile** field to the appropriate associated application profile name to define. This should be the profile from the previous screen.

  (c) Set the **Detail: Description** field to a meaningful description for this application profile record.

  (d) Set the **Detail: Scope** field to **NO SCOPE** for this and all profile records.

  (e) Set the **Detail: Flags** field to appropriate flag names that will be passed values by the user when using this application-related profile. For Navy applications, enter **Y** in this field to indicate an **activity code** is required by this application, or leave blank if the application does not require an **activity code**.

(f) Set the **Detail: Disabled** field to **N** (to enable access to this user profile record).

Use the **BOSS Configuration Subsystem Domain BOSSID File Maintenance** screen **[F4]** to define the domain member userids and link them to prospective domains in BOSS by doing the following:

(1) Set the **Domain Name** field to the name of the domain to update.

(2) Set the **BOSSID Group** field to the groupname of the users to make a member of this domain.

(3) Set the **BOSSID User** field to the userid of the specific user to make a member of this domain.

o. Verify that BOSS is properly configured, the supporting BOSS database is loaded with the appropriate information (user, terminal, application, linkage, remote node, domain, advanced auditing, etc.), and that BOSS is properly functioning by providing the appropriate security and generating the appropriate audit data.

This can be accomplished by random testing of user access through BOSS after configuration and loading are completed. Following the test, review the BOSS audit data as well as the results of the testing. Further detailed verification can be accomplished by dumping the database as formatted reports, and comparing the information in those reports against the appropriate DAC and/or user I&A requirements scheduled to be loaded into BOSS at the site.

p. Use the **BOSS Utilities Password Change Utility** screen to secure the BOSS software after configuration and testing are complete by doing the following:

(1) Enter the group (BOSS), the name (MAINT), and a new password, and then validate the new password. Then press the F1 function key to change the password. Write it down and lock it up.

(2) Update the normal system startup obeys files to include the appropriate commands necessary to start the BOSS Pathway system. The BOSS Pathway needs to be started after starting the global system-level resources (e.g., TM/MP, MEASURE subsystem, Safeguard, Spooler, tape label processing, NetBatch, etc.) prior to starting any other Pathway system, and prior to starting the TCP/IP Telnet windows.

APPENDIX F. “HOW TO” GUIDE FOR CMON

Implement CMON (command interface monitor).

Install and test the SSO-written, FSO-approved CMON program to secure and audit TACL users according to security requirements.

Build $CMON startup and auditing configuration obey files.

Build $CMON supporting database files.

Update appropriate system startup files to include the $CMON process.

Secure $CMON to only run under SUPER.SUPER.

TACL

```
TACL>LOGON SUPER.SUPER, <pswd>
TACL>FUP GIVE $SYSTEM.CMON.*, 255,255
TACL>FUP SECURE $SYSTEM.CMON.*, "OOOO"
TACL>RUN <CMONOBJ>/NAME $CMON, NOWAIT, CPU 0/1
```

SAFEGUARD

```
TACL>SAFECOM
                         = PROCESS $CMON, OWNER 255,255
```

APPENDIX G. "HOW TO" GUIDE FOR SNMP

Start SNMPAGT.

RUN SNMPAGT /NAME $agent-process, NOWAIT/

The <$agent-process> normally starts with $ZTS.

NOTE: The above agent needs to be started before the Trap Multiplexer is started.

Start the Trap Multiplexer.

Syntax.

RUN SNMPTMUX /NAME $ZTMX, NOWAIT/ -t ($ZTC0, $ZTC1)

NOTE: Known problems can be found in the TIM documentation under "Known Problems Remaining:" in the SNMP Trap Multiplexer document.

The process will abend if it is started after 18 January 2038.

The following is information gathered from the help in the SCF utility on the Tandem.

SCF>help SNMP

The NonStop agent is an SNMP agent process that performs network management operations on behalf of an SNMP manager. The NonStop agent forwards requests to appropriate subagents that translate SNMP requests into subsystem commands and subsystem responses into responses that the SNMP manager can recognize. The NonStop agent accepts requests from and sends responses and traps to one or more SNMP manager stations.

The SCF commands and applicable NonStop agent object types are summarized in the following table.

Cmd/Obj	End Point	NULL	Process	Profile	Trap dest
Abort	X			X	X
ADD	X			X	X
ALTER	X		X	X	X
DELETE	X			X	X
INFO	X		X	X	X
NAMES		X	X		
START	X			X	X
STATUS	X		X	X	X
STOP	X			X	X
TRACE			X		
VERSION		X	X		

Check to see if SNMP is running on the Tandem.

To check to see if SNMP is running on your system, you can check in several ways. One of those ways would be using SCF.

SCF is the utility for managing the network. This utility will be secured so only the system administration group can access it. This is to ensure that dynamic changes are not made to the communications with the Tandem. When a Cold Load (Reboot) is done, all dynamic changes that have not been put into the configuration files will be lost.

- The IAO, in conjunction with the SA, will ensure that the SNMP communications information is checked on a period schedule to ensure the consistency with the SNMP start up files.

- The IAO, in conjunction with the SA, will ensure that the SNMP configuration and associated files are secured so only the System Administration Group can access them, to include but not limited to the following:

  Supporting UDP Only:

  SNMPGT
  SNMPTRAP
  SNMPMON

Supporting UDP and IPC:

SNMPGET
SNMPNEXT
SNMPSET
SNMPWALK
SNMPHOST

Check the SNMP information using SCF.

```
TACL>SCF
SCF>INFO PROCESS $*

SNMP Info PROCESS

Name          *EMS Collector
$ZTMXA        \TANDEM.$0

SNMP Info PROCESS

Name          *EMS Collector
$ZTSMS        \TANDEM.$0
```

After you get the extracted information above, you will look for the process name and issue the following command. This will give you detailed information on the process and all the subs.

You will be looking for the Program file name, so you will know the location of the executable. You will need to check the security and owner of the program to ensure that the System Administrator is the owner and the security is “OOOO”.

You will also need to check the community to ensure that it is not “public”, “private”, or any default setting.

SCF>info process $ztmxa,sub,detail

```
SNMP Detailed Info PROCESS \TANDEM.$ZTMXA

 Program file name...... \TANDEM.$SYSTEM.SYSTEM.SNMPAGT
 Swap volume............ $SYSTEM
*EMS Collector.......... \TANDEM.$0
```

```
SNMP Detailed Info PROFILE \TANDEM.$ZTMXA.#DEFAULT

*Access................. READONLY
*Hostaddr............... 192.168.1.1
*Community.............. public

SNMP Detailed Info ENDPOINT \TANDEM.$ZTMXA.#DEFAULT

*Network................ \TANDEM.$ZB012
*Hostaddr............... 0.0.0.0
```

NOTE: You can then check the status of the next SNMP processing that was identified above.

```
>info process $ztsms,sub,detail
```

```
SNMP Detailed Info PROCESS \TANDEM.$ZTSMS

 Program file name...... \TANDEM.$SYSTEM.SYSTEM.SNMPAGT
 Swap volume............ $SYSTEM
*EMS Collector.......... \TANDEM.$0

SNMP Detailed Info PROFILE \TANDEM.$ZTSMS.#DEFAULT

*Access................. READONLY
*Hostaddr............... 0.0.0.0
*Community.............. public

SNMP Detailed Info PROFILE \TANDEM.$ZTSMS.#TSMPRI

*Access................. READWRITE
*Hostaddr............... 192.168.1.2
*Community.............. {Community Password}

SNMP Detailed Info ENDPOINT \TANDEM.$ZTSMS.#DEFAULT

*Network................ \TANDEM.$ZTCP0
*Hostaddr............... 0.0.0.0

SNMP Detailed Info ENDPOINT \TANDEM.$ZTSMS.#TSMEND

*Network................ \TANDEM.$ZTCP1
*Hostaddr............... 0.0.0.0
```

SNMP Detailed Info TRAPDEST \TANDEM.$ZTSMS.#TSMPRI

*Network................ \TANDEM.$ZTCP0
*Hostaddr............... 192.168.1.2
*Community.............. {*Community Password*}

SNMP Detailed Info TRAPDEST \TANDEM.$ZTSMS.#TSMPRIB

*Network................ \TANDEM.$ZTCP1
*Hostaddr............... 192.168.1.2
*Community.............. {*Community Password*}

NOTE: The community name is the same thing as a password. If others are able to guess the password, for example having Public or Private as the default "passwords", then the defaults "Public" and "Private" should be changed.

Check the SNMP information using STATUS.

First you will need to find the modules that are on the system associated with SNMP. You can do this by issuing the following command:

```
FILEINFO $*.*.*SNMP*
```

This will get you the objects on the system. Once this is done, you can issue the following command to see if they are running.

```
STATUS *,PROG $<Volume>.<Subvolume>.<Program Name>
```

If nothing reports back, then there is no process running on the system that uses this program. Repeat for any other programs that were reported above.

Start snmphost manager.

```
snmphost /name $mymgr/ -d 5 -c "MyCommunityName" -p 161 SomeSys
```

For more information, check the TIM documentation for detailed information on starting, monitoring, etc., of the SNMP processes and modules.

This page is intentionally left blank.

APPENDIX H. DOD-CERT

When vulnerabilities are discovered, the DOD-CERT Branch displays IAVM notices on their web site (**http://www.cert.mil**).

NOTE**:** **Cert.mil** only accepts anonymous FTP connections from **.mil** addresses that are registered with the Network Information Center (NIC) or DNS. If your system is not registered, you must provide your **.mil** IP address to DOD-CERT before access can be provided

The Assessments Department develops and maintains automated tools for vulnerability assessments, and analyzes and develops countermeasures to tools used by intruders. The Assessments Department also provides expert technical INFOSEC support to criminal and counter-intelligence investigations. Included within the Assessments Department is the Security Services Branch, which manages the INFOSEC Technical Services Contract.

DOD-CERT Contact Information:

PHONE: 800-357-4231
COMM 703-607-4700, DSN 327-4700
ELECTRONIC MAIL: **cert@cert.mil**
FAX: COMM 703-607-4735, DSN 607-4735, Secure 703-607-4001

It is strongly recommended that all IAOs and SAs regularly browse the DOD-CERT web page (URL: **http://www.cert.mil**). Bulletins of interest may be found in the following locations:

- **CERT/CC** is the commercial CERT Coordination Center. Their home page is **http://www.cert.org.**

- **CIAC from DOE** may be a resource for information. Their home page address is **http://www.doe.gov**. Then access the CIAC section or use the URL: **http://ciac.llnl.gov**.

- **FedCIRC** Security Resources Home Page may be a resource for information. Their address is **http://fedcirc.llnl.gov**.

This page is intentionally left blank.

APPENDIX I. IAVM/VCTS COMPLIANCE

THE CUTOFF DATE FOR IAVAs COVERED IN THIS STIG IS 24 February 2003.

The Tandem vulnerabilities listed and summarized below are covered within this version of this STIG. All IAVM program notices require appropriate action by the SA, if applicable. The SA must update the VCTS asset entry with the action taken to address each issued IAVM program notice. This action would consist of checking and fixing the system and updating of the system entry in VCTS. All IAVM program notices (this includes Alerts, Bulletins, and Technical Advisories) are subject to review by Security Readiness Review Teams.

***NOTE*:** Additional vulnerabilities may have been released since the publication of this STIG. Each site should routinely check the IAVM/CERT for subsequent bulletins concerning the Tandem operating system. A VCTS, VS08 OS Vulnerability Summary Report, will provide a list of Tandem vulnerabilities (similar to below), which require action by the SA. Any new IAVA vulnerabilities, not listed here, are also subject to review by Security Readiness Review Teams.

VS08 – OS Vulnerability Summary Report

OS: Tandem-Guardian

NO.	VULNERABILITY	VULNERABILITY DESCRIPTION	BULLETIN RELEASE DATE	APPLICATION
1.	**2000-A-0001.0.0-01**	Cross-site Scripting Vulnerability	02 Feb 2000	Web Servers and Browsers
2.	**2000-B-0001.0.0-01**	BIND NXT Buffer Overflow	06 Mar 2000	DNS BIND
3.	**2000-B-0003.0.0-01**	Multiple Buffer Overflows in Kerberos Authenticated Services	24 May 2000	Kerberos
4.	**2000-T-0006-01**	Frame Domain Certification, Unauthorized Cookie Access and Malformed Component Attribute Vulnerabilities	24 May 2000	Microsoft Internet Explorer
5.	**2000-B-0008.0.0-01**	BIND 8.2.2-P6 Denial of Service Vulnerabilities	14 Nov 2000	DNS BIND
6.	**2001-A-0001.0.1**	Multiple Vulnerabilities in BIND	15 Feb 2001	DNS BIND
7.	**2001-B-0003-01**	%U Encoding Intrusion Detection System Bypass Vulnerability	15 Oct 2001	IDS Software
8.	**2001-T-0009-01**	Symantec Norton Antivirus LiveUpdate Host Verification Vulnerability	24 Oct 2001	Antivirus Software
9.	**2001-T-0018-01**	Short Password Vulnerability in SSH Communications Security	13 Dec 2001	Secure Shell
10.	**2002-B-0003-01**	Multiple Vulnerabilities in PHP	19 Aug 2002	Web
11.	**2002-T-0004-01**	Kerberos Telnet Protocol Vulnerability	15 Mar 2002	Kerberos
12.	**2002-T-SNMP-003-01**	Multiple Simple Network Management Protocol Vulnerabilities in Servers and Applications	11 Apr 2002	SNMP Protocol

Figure I-1: VS08 – OS Vulnerability Summary Report Example

SUMMARY OF TANDEM IAVA VULNERABILITIES

NO.	IAVA NUMBER	TANDEM STATUS	REFERENCE(S)
1.	**2000-A-0001.0.0-01**	Not Applicable on DISA Tandems	Web servers can be configured on the Tandem System, but are not currently configured on the DISA Tandems. For more information on configuring a web server on a Tandem platform, refer to the Tandem TIM documentation. Because the web server is not configured, this vulnerability does not pertain to DISA Tandem Systems.
2.	**2000-B-0001.0.0-01**	Not Applicable on Tandems	DISA Tandems do not run DNS BIND software
3.	**2000-B-0003.0.0-01**	Is not available for Tandem until D48.00	Kerberos may be used on the Tandem and/or within applications. For Tandems supporting the service of Kerberos, refer to *Section 8.6.1, Kerberos (Network Authentication Protocol),* in this STIG for more information.
4.	**2000-T-0006-01**	Not Applicable on Tandems	Tandem does not run Microsoft Internet Explorer software.
5.	**2000-B-0008.0.0-01**	Not Applicable on Tandems	BIND 8.2.2-P6 Denial of Service Vulnerabilities. Tandems do not run DNS BIND software.
6.	**2001-A-0001.0.1**	Not Applicable on Tandems	Overflow in ISC BIND (DNS). Tandems do not run DNS BIND software.
7.	**2001-B-0003-01**	Not Applicable on Tandems	IDS – Not applicable to Alert + on Tandem.
8.	**2001-T-0009-01**	Not Applicable on Tandems	Norton Antivirus does not run on the Tandem.
9.	**2001-T-0018-01**	Applicable when Unix is run on the system.	If Unix is installed on the Tandem system and before starting the system , refer to the IAVA for further information
10.	**2002-B-0003-01**	Applicable	If a Web server is installed on the Tandem system, refer to IAVA 2002-B-0003-01 for additional information before connecting the system up on the network

NO.	IAVA NUMBER	TANDEM STATUS	REFERENCE(S)
11.	**2002-T-0004-01**	Applicable when using D48 or newer.	Kerberos was introduced to Tandem in the D48 version of the Kernel Software. Even if at least D48 is installed on the system, the application needs to be coded to issue the appropriate Kerberos calls.
12.	**2002-T-SNMP-003-01**	Not Applicable on Tandems	This particular IAVM is not applicable to the Tandem however 2002-A-SNMP-003-01 is applicable, to a certain degree. Please refer to paragraph 8.8.3, SNMP, for specific information on this vulnerability.

Figure I-2: Summary of Tandem IAVA Vulnerabilities

APPENDIX J. EXAMPLES OF POTENTIAL SECURITY ATTACKS

TYPES OF ATTACKS

SOCIAL ENGINEERING

Examples

- Attacker calls switchboard and impersonates employee, "This is Mr. Jones trying to reach the data center, can you transfer me to the data center? " (Data Center) This is Mr. Jones, my modem is not working, has the modem pool phone number changed?" (Gets modem pool phone number and name of the system manager from the data center operator.) Calls computer room. "This is <system manager>; I've forgotten my password. Can you reset it for me?" Attacker dials into the system, and logs on as a valid user.

- Attacker causes CPU halting by executing the tool DIVER.

- Attacker logs on from a remote node as a local userid and acts as a local user.

Protection Strategy

- Educate users and staff.

- Require the use of **validation** code words that would only be known to the user for further identification. This is available through the BOSS User Directory Services feature.

- Secure DIVER and other tools to prevent use by unauthorized users.

- Do not give out phone numbers or access information over the telephone.

- Do not use userids that can be easily guessed.

DATA DRIVEN ATTACKS

Examples

- Attacker obtains data by access to spooled output, reports, or file copies (data monitoring of printed reports, perusing of spooled output, or microfiche reports).

- Attacker modifies data by obtaining access to the data (either from tape or disk media) and access to system management tools such as the following:

  - **TANDUMP** (the Physical Disk Volume Dumping tool)
  - **MD2** (the Physical CPU Memory Dumping/Modification tool)
  - Any of the file data dumping tools (FUP, SQLCI, 4th GL DBMS tools, etc.)
  - SNOOP (the TM/MP Transaction Audit Log data perusing tool)
  - The applications program debugger SAVEABEND dumps
  - Inspect/debug process prompts

Protection Strategy

- Secure and destroy old data file copies and reports to prevent unauthorized user access.

- Secure tools to prevent use by unauthorized users.

- Store tape backup media in a secured facility.

- Remove Inspect symbols from production object programs.

- Address all program abort SAVEABEND dump files and purge them as soon as possible.

INFRASTRUCTURE ATTACKS

Examples

- Attacker obtains a valid user's logon by use of data scopes, LAN Analyzer, and sniffers on the lines.

- Attacker introduces line noise, causes excessive data errors hoping support staff will lower their guard on the noisy line and potentially disrupt service or steal data.

- Attacker obtains a valid user's logon by access to communications application traces or software trace data.

- Attacker modifies system configuration by the use of the dynamic system configuration modification tool, COUP, communications configuration/modification tools, CUP, CMI, SCF, and NETCOM, or the I/O device configuration table tool, MIO. Attacker causes system outage.

Protection Strategy

- Store diagnostic tools (i.e., data scopes, LAN Analyzer, and sniffers) in a secured facility.

- Secure trace tools to prevent use by unauthorized users.

- Secure trace output data, and delete old trace data files to prevent use by unauthorized users.

- Prevent access to communications lines in places where data scopes, LAN Analyzer, and sniffers can be put on the lines.

- Use caution (delete user and password information in trace file) when sending trace data off-site for analysis.

- Use caution when making modifications to communications lines to address line noise.

- Maintain the TCB in a secured facility.

This page is intentionally left blank.

APPENDIX K. SOFTWARE PRODUCTS THAT REQUIRE FURTHER RESEARCH

- The ENLIGHTEN COTS product
- The New Dimension Software, Inc. CONTROL-M and CONTROL-R (Tandem Performance Monitor) COTS products
- The New Dimension Software, Inc. CONTROL-O COTS product
- The MAXM Systems MAX/Enterprise COTS products
- Compaq/Tandem, Java Virtual Machine and Java Development Kit 1.1.2 SERVLET application program interfaces for ITP Web Server package
- The OMNIGUARD COTS products
- The TAPES MANAGER COTS product
- The QTOS COTS product
- Intrusion detection software (e.g., Alert Plus)
- Commence (old TIC sold by MAXM)

This page is intentionally left blank.

APPENDIX L. POTENTIAL SECURITY EXPLOITS AND VULNERABILITIES

Tandem NonStop Kernel Potential Security Exploits and Vulnerabilities

Problems/Concerns Requiring Further Investigation

PROBLEM/CONCERN	***STATUS***
System cold load	This should be limited to the SA only.
CPU halting tool, DIVER	This should be limited to the SA only
Memory dumping / modification tool, MD2	This should be limited to the SA only
System configuration tools (Install, SYSGEN)	This should be limited to the SA only
Dynamic system configuration and modification tool, COUP (When using COUP, use the **LOG** command to create an audit of the commands entered by the System Administrator while using this tool.)	This should be limited to the SA only
Communications configuration/modification tools, CUP, CMI, and SCF	This should be limited to the SA only
I/O device configuration table tool, MIO	
System console, OSP/RMI	The console should be in a secured area, such as a computer floor
Data dumping tools (TANDUMP, Data Scope, Trace facility, Sniffer, LAN Analyzer) SCF	This should be limited to the SA only
Customization files (Custom 6100 CLIP Code, TACLCSTM, SCFCSTM, CMICSTM)	

PROBLEM/CONCERN	***STATUS***
Labeled tape processing and tape management software	
Program/process debuggers (Inspect/Debug)	
When processes try to perform illegal functions (disallowed by the operating system), Debug or Inspect traps halt them and their memory can be dumped to a SAVEABEND trace file, or it can be real-time accessed.	
Data file/database tools (SQLCI, FUP, RDF, BACKUP/RESTORE, TM/MP audit trails)	
Hardware tools (PUP, AID, EMS collectors/filters/distributors [EMSDIST], and TMDS)Potential processing loopholes include PROGID programs, privileged code, and licensed programs	
Backup tape data is not encrypted, but is written in a proprietary format.	

APPENDIX M. COTS PRODUCT SECURITY

Block Mode Operating Systems Services (BOSS)

The COTS product, BOSS Version 4.0, (as defined in the BOSS documentation) is configured to execute under the Super.Super userid and with file security as follows as a minimum DISA requirement:

FILE NAME	*DESCRIPTION*	*CODE*	*EOF*	*BINDER TIMESTAMP*	*VERSION PROCEDURE*	*SECURED*	*FILE TYPE*
APISRV	Server specifically for CyberBoss	100		10JUN1999 16:58:48 or 22FEB1999 12:56:11	T9999D30-40K-BOSSAPI-07JUN1999 or T9999D30-40K-BOSSAPI-22FEB1999	AGOO	Server
APLIST	Applications List File for $JR	100				AGOO	
APMENU	Application Menu File for $JR	0				AGOO	
APPFLAGS	Application Flags File (AAA)	0				AGOO	Database
APPINFO	Application Information File	0				AGOO	Database
APPINFO0	Alternate Key File for AppInfo	0				AGOO	Database Alternate Key
APPLOGO0	Alternate Key File for Applogon	0				AGOO	Database Alternate Key
APPLOGON	Application Logon File	0				AGOO	Database
ASSIGNF	Application Info. / Assign File	0				AGOO	Database
ASSIGNS	File that stores BOSS Assigns	0				AGOO	Database
BINDLIB	TACL File that checks Node Names	101				AGOO	

FILE NAME	*DESCRIPTION*	*CODE*	*EOF*	*BINDER TIMESTAMP*	*VERSION PROCEDURE*	*SECURED*	*FILE TYPE*
BINDTCP	Calls Bindlib File	101				AGOO	
BLOGNNNN	BOSS Logs (location via BOSSENV)	1001A				OOOO	Log
BOSSCOD	BOSS Physical Instruction File (Scobol)	301				AGOO	
BOSSCOLD	BOSS Startup File	101				OOOO	Obey
BOSSCOM	BOSSCOM Utility	100		22FEB1999 15:19:32	T9999D30_16Feb1999_BOSSCOM or T9999D30_4_0_03_BOSSCOM	OOOO	Utility
BOSSCONF	BOSS Configuration File	101				OOOO	Configuration.
BOSSCTL	BOSS P/W Control File	310				AGOO	
BOSSDDL4	BOSS DDLs	101				AGOO	
BOSSDIR	BOSS SCOBOL Directory	300				OOOO	
BOSSDOC	The BOSS Manual	0				AGOO	
BOSSENV	BOSS Environment File	0				AGOO	Database
BOSSID2	BOSS User ID File (Users, P/W's)	0				AGOO	Database
BOSSID20	Alternate Key File to BOSSID2	0				AGOO	Database A

FILE NAME	*DESCRIPTION*	*CODE*	*EOF*	*BINDER TIMESTAMP*	*VERSION PROCEDURE*	*SECURED*	*FILE TYPE*
BOSSMAC	BOSS Macro File ($system.system)	101				AAAO	Utility
BOSSPRGS	Programs File that is called by BOSSCONF	101				OOOO	Obey
BOSSSVRS	Servers File that is called by BOSSCONF	101				OOOO	Obey
BOSSSYM	BOSS Symbols File	302				OOOO	
BOSSTCPS	TCPs File that is called by BOSSCONF	101				OOOO	Obey
BOSSTRMS	Term File that is called by BOSSCONF	101				OOOO	Obey
BOSSUTIL	Utility File (Startup, New BOSS, etc.)	101				OOOO	Obey
BOSSUTLS	TACL Macro called by BOSSUTIL	101				OOOO	Obey
CICOMMD	Adv. Auditing at CICommand Level	0				AGOO	Database
CIPROFIL	Adv. Auditing at CIProfile Level	0				AGOO	Database
CLFPROG	Advanced Auditing Program File	100		17MAR2000 02:12:09	T9999D30^BOSS^5^0	AGAO	Database
COBLIB	BOSS COBOL Library File	101				OOOO	
COMSRV	BOSS Comm. Server (loss sessions)	100P		10JUN1997 15:42:38	T9999D30-4-0-COM-SERVER	AGOO	Server

FILE NAME	***DESCRIPTION***	***CODE***	***EOF***	***BINDER TIMESTAMP***	***VERSION PROCEDURE***	***SECURED***	***FILE TYPE***
CONVERT	BOSSUTIL 3.X to 4.0 Conv. Utility	100	52188	13OCT1999 02:49:41	>> NO T9xxx PROC <<	AGOO	Obey
DBSERVER	The BOSS Database Server	100	47104	23JUL1993 02:05:38	T9154D20^01JUN93^PATHMAKR	AGOO	Server
DOAPPID	The Domain Appl-ID File	0				AGOO	Database
DOMAIN	The Domain File	0				AGOO	Database
DOPROF	The Domain Profile File	0				AGOO	Database
DOUSER	The Domain User File	0				AGOO	Database
EXECSRV	BOSS Executor Server	100L		18MAY1999 15:26:39	T9999D30^BOSS^4^0K	AGOO	Server
FIXFILE	Allows Fix of Text Base Fields	100				AGOO	Utility
FUNCTION	BOSS Function File (AAA)	0				AGOO	Database
HELPALT0	Help Alternate Key File	210				AGOO	Help
HELPPOS	Help Position File	210				AGOO	Help
HELPREQ	Help Requester	210				AGOO	Help
HELPSRV0	Help Alternate Key File	100		23JUL1993 03:52:18	T9154D20^01JUN93^PATHMAKR	AGOO	Help
HELPTXT	Help Text File	210				AGOO	Help
HELPTXT0	Alternate Key File for HelpTxt	210				AGOO	Help

FILE NAME	*DESCRIPTION*	*CODE*	*EOF*	*BINDER TIMESTAMP*	*VERSION PROCEDURE*	*SECURED*	*FILE TYPE*
JRCOD	$JR Test Pathway	301				AGOO	$JR
JRCOLD	$JR Coldstart File	101				OOOO	$JR
JRCONF	$JR Config. File	101				OOOO	$JR
JRCTL	$JR Control File	310				AGOO	$JR
JRDIR	$JR Directory File	300				AGOO	$JR
JRLOG	$JR Log	0				AGOO	$JR
LISTSRV	The BOSS List Server	100		08NOV1998 22:25:35	T9999D30-4-0C-LIST-SERVER	AGOO	Server
LOCATE	Locate Utility (who's where?)	0				AGOO	Database
LOCATE0	Alternate Key File for Locate	0				AGOO	Database Alternate Key
LOCSRV	The Locate Server	100		27MAY1998 04:16:46	T9999D30-4-0-LOCATOR-SERVER	AGOO	Server
LOGONSRV	The Logon Server	100		13MAR2000 13:38:56	T9999D30-5-0-BOSS-LOGON	AGOO	Server
MENU2	BOSS Menu File (links Progs. To Users)	0				AGOO	Database
PARAMS	File that holds BOSS Params	0				AGOO	Database
PARMFILE	Appl-Info Parameter File	0				AGOO	Database
PASSHIST	Password History File	0				AGOO	Database

FILE NAME	*DESCRIPTION*	*CODE*	*EOF*	*BINDER TIMESTAMP*	*VERSION PROCEDURE*	*SECURED*	*FILE TYPE*
PASSLINK	P/W Link (from BOSS to NSK)	100				AGOO	
PATHINFO	BOSS P/W Info File	0				AGOO	
PATHTCP2	Pathway TCP Control File	100/700				AGOO	
PLINKSRV	The Pathlink Server	100P		15FEB2001 16:16:22 or 03SEP1999 02:37:04	T9999D40-5-0-PATHLINK-SERVER or T9999D30-4-0C-PATHLINK-SERVER	AGOO	Server
PROFDET	Application Profile Maint. Detail File	0				AGOO	Database
PROFILE	Application Profile Maint. File	0				AGOO	Database
PROMPT	BOSS Prompt File ($system.system)	100		28JUL1989 12:12:01	>> NO T9xxx PROC <<	AAAO	Utility
RESETEFF	Reset EFF utility (to reset Passwords)	100				AGOO	Utility.
SCOPE	Scope (affiliated with Domain)	0				AGOO	Database
SCOPEDET	Scope Detail File	0				AGOO	Database
SECPROG	Utility To Grant User's Privileges	100L				AGOO	Utility
SECSRV	The BOSS Security Server	100P		12MAR2000 19:47:03	T9999D30-4-0K-SEC-SERVER	AGOO	Server

FILE NAME	*DESCRIPTION*	*CODE*	*EOF*	*BINDER TIMESTAMP*	*VERSION PROCEDURE*	*SECURED*	*FILE TYPE*
SETEFF	Set EFF utility (Set Eff. Date for P/W's)	100				AGOO	Utility
TALPROC	TAL Procedures File	100				AGOO	
TCPL2	Library created by BINDTCP (node rel.)	100				AGOO	
TERMLANG	File that is linked to TERM (language)	0				AGOO	Database
TERMS	Terminals File	0				AGOO	Database
TITLE	Title File	0				AGOO	Database
TOKEN	File that controls Token(s)	0				AGOO	Database
TOKEN0	Alternate Key File For Token	0				AGOO	Database Alternate Key
USELOGSP	ENFORM Report	101				AGOO	
USELOGSS	ENFORM Report	101				AGOO	
USEMENU	ENFORM Report	101				AGOO	
USERCOMD	User Command File	0				AGOO	Database
USERDET	User Detail File	0				AAOO	Database
USERDET0	Alternate Key File for UserDet	0				AAOO	Database Alternate Key
USERNODE	File that tracks User/Node access	0				AGOO	Database

FILE NAME	*DESCRIPTION*	*CODE*	*EOF*	*BINDER TIMESTAMP*	*VERSION PROCEDURE*	*SECURED*	*FILE TYPE*
UTILSRV	BOSS Utility Server	100		31AUG1999 01:52:43	T9999D30-4-0C-UTILITY-SERVER	AGOO	Server
VPTSRV	BOSS Viewpoint Server	100				AGOO	Server

NOTE 1: Newer versions of this product may supplement this list with new requirements. This Appendix will be updated for the next release of this STIG.

NOTE 2: The file codes are defined as follows:
100 - Program
101 - Edit file
300 – Scobol directory file
301 – Scobol requestor code
302 – Scobol Inspect Symbols file
310 – Pathway used control file
700 – Program
1001 – BOSS logfiles
0 - Entry sequenced file (Fixed Length records)
L – Indicates the program is licensed
P - Indicates the program has the PROGID bit set

APPENDIX N. GOTS PRODUCT SECURITY

Command Interpreter Monitor (CMON)

The GOTS product CMON, Version 02-00, is configured to execute under the Super.Super userid and with file security as follows:

$SYSTEM.CMON

NOTE**:** The CMON files should be secured to the owner of Super.Super (255, 255)

FILE NAME	***DESCRIPTION***	***CODE***	***EOF***	***BINDER TIMESTAMP***	***VERSION PROCEDURE***	***SECURED***	***FILE TYPE***
CMONCTRL		101	2280			OOOO	
CMONLOG		0	0			OOOO	
ES1CMONO		100P	132442	11JAN2000 09:09:39	T9000D39_02^ VERSION^11JAN00	OOOO	
ES8HEYO		100	103196			OOOO	
ES8SRVO		100	32868			OOOO	
HEYCMON		100	56604	11JAN2000 09:10:19	T9000D39^ VERSION^11JAN00	OOOO	
NOTICE		101	0			OOOO	
PROCESS		101	0			OOOO	

FILE NAME	***DESCRIPTION***	***CODE***	***EOF***	***BINDER TIMESTAMP***	***VERSION PROCEDURE***	***SECURED***	***FILE TYPE***
RUNCMON		101	2906			OOOO	
SOFTDOC		101	40222			OOOO	
TCMONLOG		0	0			OOOO	

N*OTE1*: The file size (EOF) may vary depending on the CMON version.

NOTE2: Newer versions of this product may supplement this list with new requirements. This Appendix will be updated for the next release of this STIG.

***NOTE3*:** The file codes are defined as follows:
100 - Program
101 - Edit file
0 - Entry sequenced file (Fixed Length records)
P - Indicates the program has the PROGID bit set

APPENDIX O. TANDEM PROGRAMS TO BE AUDITED

ADDUSER

AID

AXCEL

BACKUP

BACKUPCPU

BIND

BOSS (BOSSCOM)

C

CMI

CMON

CMP

COBOL

COBOL85

COMINT

COUP

CROSSREF

CUP

DDL

DEBUG

DELUSER

DCOM

DISKGEN

DIVER

DNS

DSAP

DSC

EDIT

EMSCOLLECT

EMSDIST

ENFORM

ENLIGHTEN

EXEC

FASTSORT

FOCUS

FTP

FUP *(CREATE, DUP, GIVE, LOAD, PURGE, SECURE)*

GPA

IMON

INET

INSPECT

INSTALL

LISTENER

LITECOM

LOAD

LOGOFF

LOGON

MEASCOM

MEASMON

MD2

MIO

NETCOM

PAL

PASCAL

PASSWORD

PATHCOM

PATHMAKR

PATHMON

PATHTCP

PEEK

PERUSE

PMINSTALL

PUP *(FORMAT, REMOVE, REVIVE, UP)*

RECEIVEDUMP

RELOADCPU

REMOTEPASSWORD

RESTORE

RJECI

SAS

SCF

SCOBOL

SCOBOLX

SORT

SCUP

SPOOLCOM

STATUS

SQLCI

SQLCOMP

SWITCH

SYSGEN

TACL (FULL)

TAL

TANDUMP

TAPECOM

TCPIP

TEDIT

TELNET

TELSERV

TGAL

TIME

TMDS

TMFCOM

UPDATE

VIEWPT

VIEWSYS

XRAYCOM

XRAYSCAN

XREF

XVS

This page is intentionally left blank.

APPENDIX P. BOSS DEFAULT USERID SETTINGS

TACL MACRO Fix, Explanation Message:

A BOSS password issue has been uncovered where there are instances of a user's password being printed in the BOSS audit logfile. This will occur if a user has an audited TACL and uses the **LOGON** or **PASSWORD** command at the TACL prompt. To prevent the password from being printed in the Log, it is imperative that each site denies **LOGON** and **PASSWORD** in their CI profiles for all occurrences of TACL.

The only instance where a user would need to use the **LOGON** command at a TACL prompt in the DOD environment is a Domain Manager or a BOSSMAINT Manager adding a new user. When the Manager adds a new NSK userid, the Manager needs to log on as that user to change the Default Volume.Subvolume and the Security flags. An NSK user should never change their password at a TACL prompt. Passwords should always be changed through the BOSS Logon screen.

Use a TACL Macro from the Menu screen of the BOSS Manager or Domain Manager to set a new user’s default volume and file security. Enter **Group.Newuser $volume.subvolume XXXX** on the Menu screen:, and then select the TACL Macro. The Manager will get a TACL and will be prompted for the **Group.Newuser** password. Once that is entered, the **DEFAULT** command will execute with the given parameters. Then the Manager will be prompted to enter any key to exit. Because this is a TACL macro, the password will **not** be displayed in the BOSS audit logfile.

Group.Newuser = The new user's group and userid
$volume.subvolume = The Default volume and subvolume that you want to set for the new user
XXXX = The Default RWEP flags for the new user (i.e., "OOOO") (It is not necessary to put the "" around the flags; that is done in the TACL Macro.)

This is only needed for adding NSK Users. A BOSS Logical User does not obtain an NSK userid, and therefore does not need to have these defaults set.

SSO Mechanicsburg provided instruction (see e-mail elsewhere in this appendix) that gave detailed instructions on how to implement the TACL macro and how to use it to set the security flags for a new user without using the **LOGON** command at a TACL that would put the password into the BOSS audit logfile.

TACL MACRO Fix and Installation Instructions:

To implement the TACL Macro, add these lines to your BOSSMAC file. The BOSSMAC file either resides on your BOSS subvolume or on $SYSTEM.SYSTEM. This example uses $SYSTEM.SYSTEM.BOSSMAC. The Macro is named DEFVOLSC for DEFault VOLume.subvolume file SeCurity flags. This name must match what is entered on the command line of the Application Information File Maintenance screen.

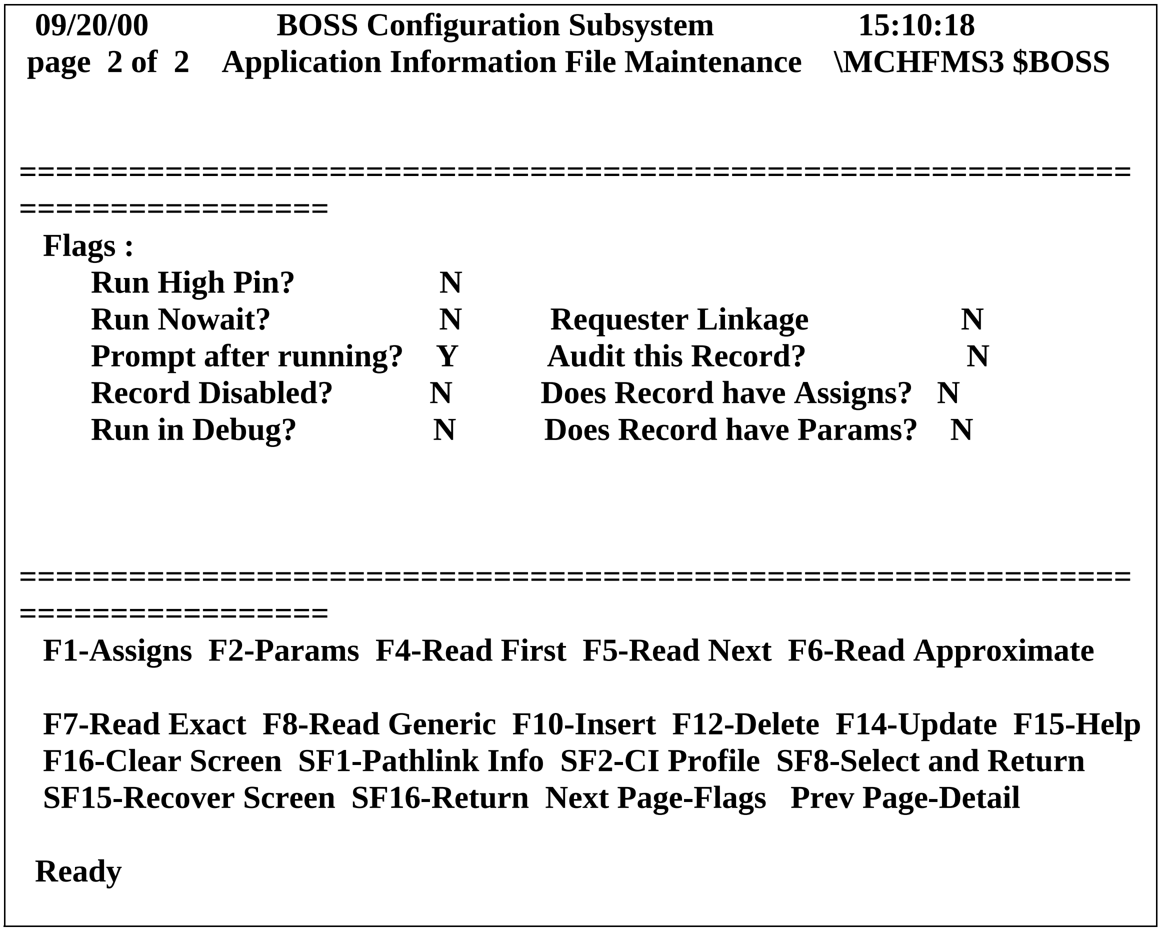
```
?SECTION DEFVOLSC MACRO
===================
====DEFVOLSC=====
===================
LOGON %1%
DEFAULT %2%,"%3%"
```

Add DEFVOLSC to the BOSS Application Information Screen as follows:

```
09/20/00             BOSS Configuration Subsystem              15:05:42
 page  1 of  2    Application Information File Maintenance    \MCHFMS3 $BOSS



=============================================================
=================
 * Program ID      DEFVOLSC

   Menu Description DEFAULT SECURITY MACRO FOR NEW USERS

   Object          $SYSTEM.TACLHIGH.TACLDMGR

   Input File Name  $RECEIVE
   Output File Name
   Command Line     SINK [#LOAD/KEEP
1/$SYSTEM.SYSTEM.BOSSMAC]~;AUTO &~; DEFVO
      LSC % ~;EXIT

   Type of Object     I            Run As:
   Run Time Priority     0
   CPU to use
   Startup Volume  :          Startup Subvol :

=============================================================
=================
   F1-Assigns  F2-Params  F4-Read First  F5-Read Next  F6-Read Approximate

   F7-Read Exact  F8-Read Generic  F10-Insert  F12-Delete  F14-Update  F15-Help
   F16-Clear Screen  SF1-Pathlink Info  SF2-CI Profile  SF8-Select and Return
   SF15-Recover Screen  SF16-Return  Next Page-Flags   Prev Page-Detail

  Record read OK                Approx  key Application ID
```

You can make the Menu Description meaningful for you!

Application Information Record:



```
 09/20/00            BOSS Configuration Subsystem            15:10:18
page  2 of  2    Application Information File Maintenance    \MCHFMS3 $BOSS



=============================================================
=================
  Flags :
      Run High Pin?               N
      Run Nowait?                 N         Requester Linkage              N
      Prompt after running?    Y          Audit this Record?               N
      Record Disabled?           N         Does Record have Assigns?   N
      Run in Debug?               N         Does Record have Params?    N




=============================================================
=================
  F1-Assigns  F2-Params  F4-Read First  F5-Read Next  F6-Read Approximate

  F7-Read Exact  F8-Read Generic  F10-Insert  F12-Delete  F14-Update  F15-Help
  F16-Clear Screen  SF1-Pathlink Info  SF2-CI Profile  SF8-Select and Return
  SF15-Recover Screen  SF16-Return  Next Page-Flags   Prev Page-Detail

 Ready
```

After adding the lines to BOSSMAC and adding the Application Information Record, add the TACL Macro to the Domain Manager's Menu. Try it on your own menu to make sure it works for you. Once it is on your menu, use the screen example of how to execute it. This is an example of the User's Menu screen:

```
09/20/00    DEPARTMENT OF DEFENSE INTEREST COMPUTER SYSTEM
(DODICS)  15:16
                  Available Program Menu          \MCHFMS3 $BOSS
============================================================
=================
         Record                    Description
     --------------------           --------------------------------------
  F1  PRTREST                   -> PRINTER RESTART MACRO

  F2  TACL255                   -> TACL which RUNS AS 255,255
  F3  DEFVOLSC                  -> DEFAULT SECURITY MACRO FOR NEW
USERS
  F4  LOGONMAC                  -> LOGON MACRO
  F5  TACL                      -> Tandem Advanced Command Language

  F6  TACLLKB                   -> Audited TACL
  F7  EDITA                     -> EDIT that is AUDITED
  F8  TERM RESTART $BOSS-> TERMINAL RESTART FOR TERMINALS
IN $BOSS
  F9  TRMRST                    -> TERMINAL RESTART MACRO

  F10 TACLIXF                   -> TACL for IXF only - no other commands


      APPLP.DAZ0999 $DATA1.DAZ0999 OOOO
                              2  OF  3
============================================================
==================
 Press function key to run prog     User     MCHFM3
 SF1 for next page, SF2 for prev page,       DAZ0520
 SF3 for base menu, SF16 to exit, F16 Network Select  Term     BOSS26
```

Enter the new User's ID, Default vol.subvol, and security flags as shown above and then select F3 in this example. Do **not** separate the arguments with commas. The three arguments are separated with spaces.

This page is intentionally left blank.

APPENDIX Q. LIST OF ACRONYMS

Acronym	Definition
AC	Alternating electrical current, where the electrical current supplied has spikes that result in a fluctuation between a positive and negative portion in the cycle of current
ACL	Access Control List
AIS	Automated Information System
ASCII	American Standard Code for Information Interchange (a character set consisting of 7-bit coded characters and one parity check bit)
ASDC3I	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
Async	Asynchronous communications protocol
Audit Dump	Copy of a TM/MP audit trail file written to a tape or disk volume
Audit Trail	A record of system events, either printed or electronically readable, that is used to perform an audit
Auto Logoff	A process that terminates an inactive session after a preset number of minutes during which the terminal has been idle
Auto-Rollback	A TM/MP feature for restoring logically inconsistent disk files to their most recent consistent state
BOSS	Block-mode Operating System Services product
Bitsync	Bit synchronous communications protocol
Bytesync	Byte synchronous communications protocol
CAID	Creator Accessor ID used to identify the user who initiated the creation of a process
CCB	Configuration Control Broad
CDA	Central Design Activity
CLEARONPURGE	A file option that instructs Kernel to overwrite the data in a file with (binary zeros) when the file is purged

CMON	Command interpreter MONitor**:** A user-written program that monitors, audits, and controls some Command Interpreter functions
COMINT	Tandem’s older release of a COMmand INTerpreter
COTS	Commercial Off-The-Shelf
CSU	Control Service Unit
Database	Organized collection of data for a particular function
DC	Direct electrical current, where the alternating electrical cycle has been flattened, eliminating the spikes in the fluctuations between positive and negative portions in the cycle of current supplied
DCOM	Disk Compression utility program that compresses space on a disk volume
DDL	Data Definition Language
DHCP	Dynamic Host Configuration Protocol
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISAI	Defense Information Systems Agency Instruction
DMS	Defense Message System
DNS	Domain Name Service
DOD	Department of Defense
DOD-CERT	Department of Defense-Computer Emergency Response Team
DODIG	DOD Inspector General
DSAP	Disk Space Analysis Program (a utility to analyze how space on a disk volume is being used)
DSU	Data Service Unit
EMS	Event Management Service
Enscribe	Tandem’s file management system software
EXPAND	Tandem’s NonStop proprietary network that extends the concept of system to a geographically distributed NonStop system
FSO	Field Security Operations (DISA)

FTP	File Transfer Protocol (a TCP/IP service)
FUP	File Utility Program (a Tandem utility program used for file management)
GIG	Global Information Grid
GNOSC	Global Network Operations and Security Center
GOTS	Government Off-The-Shelf
GroupName	A Kernel name for a group of users who are assigned a groupnumber and have an association (e.g., **test.john**, where **test** is the groupname, and **john** is the username)
GroupNumber	A Kernel number for a group of users who are assigned a groupname, and has an association (e.g., **10.1**, where **10** is the groupnumber, and **1** is the usernumber)
HTTP	Hyper Text Transport Protocol (used for Internet communications)
I&A	Identification and Authentication
IAVM	Information Assurance Vulnerability Management
IAW	In accordance with
IEEE	Institute for Electrical and Electronic Engineers (a standards-making committee)
INFOSEC	Information Security
Install	A Tandem utility program that is used to configure and install new operating system software and to assemble an operating system image
IP	Internet Protocol
IPMs	Interim Product Maintenance Releases (problem fix)
IS	Information System
IAM	Information Assurance Manager
IAO	Information Assurance Officer
LAN	Local Area Network
Licensed	An attribute assigned by the SUPER.SUPER userid to program files on a Tandem system, which allows the execution of privileged procedure calls by non-privileged users

Macro	A sequence of TACL commands and built-in functions that can allow parameter-driven substitution to standard functions, and can be executed as a job on a Tandem system
MIB	Management Information Base
MOA	Memorandum of Agreement
MSG	Materiel Systems Group (application development group for the Air Force)
NCSC	National Computer Security Center
Node	A Tandem computer system that is part of an EXPAND network
NonStop SQL	See *NSSQL*
NSO	Network Security Officer
NSSQL	Tandem’s NonStop SQL database management system
OSP	Operations and Service Processor (for Tandem systems) (see *RMI/OSP*)
PAID	Process Accessor ID (Identifier of the userid that is used to determine the authorizations for a process. The PAID can be programmatically altered using the **verifyuser** procedure call or the PROGID program file parameter.)
Pathway	A Tandem software product that provides an operating environment for the execution of applications and multi-threaded mapping of servers to users’ terminals
PC	Personal Computer
POP	Point-of-Presence
PROGID	A program file option that changes the PAID for processes executing on a Tandem system, causing the process to have the same PAID as the program file owner
PUP	Peripheral Utility Program (a Tandem utility program used for device management)
RNOSC	Regional Network Operations and Security Center
RMI/OSP	Remote Maintenance Interface/Operations and Service Processor console device for Tandem systems that provides access to the system at a low level for diagnostics and system startup operations functions
SACS	Security Access Control System

SCF	Subsystem Control Facility
SFUG	Security Features User's Guide
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
Spooler	A set of Tandem programs that acts as an interface between the processes and the print devices for creating printed reports
SRRDB	Security Readiness Review Database. A reporting system that manages information gathered from the sites during a Security Readiness Review.
SSO	Systems Support Office (DISA Technical Systems Support group)
STIG	Security Technical Implementation Guide
Super-group	Any user whose group ID is 255. (The userids within the super-group have the authorizations [primarily related to system operations] that are not available to other users.)
Super ID	Reserved userid (255,255) for system administration. (The processes executed by this ID are considered to be **trusted** and bypass the security checks.)
SYSGEN	A utility program used by Install to generate an operating system image that binds together the operating system software and the hardware configuration for the Tandem system
TACL	Tandem's Advanced Command Language (used as both a Command Interpreter and a command language)
TASO	Terminal Area Security Officer
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TIM	(Tandem's) Total Information Manager (a series of manuals on CD-ROM)
TIM	Technical Interchange Meeting (DISA FSO STIG Discussions)
TMF	Transaction Monitoring Facility for database auditing and integrity (now a subset of TM/MP)

TM/MP	NonStop Transaction Manager/Management Process (TM/MP) (bundled software and the replacement product for TMF)
URL	Universal Resource Locator
Userid Number	A Kernel number for a user that is assigned to a username and has an association to a class of users as a user group (e.g., **10.1**, where **10** is the groupnumber and **1** is the usernumber)
Username	A Kernel name for a user that is assigned a unique userid number and has an association to a class of users as a user group (e.g., **test.john**, where **test** is the groupname, and **john** is the username)
VCTS	Vulnerability Compliance Tracking System
VMS	Vulnerability Management System
WAN	Wide Area Network
WESTHEM	Western Hemisphere
WWW	World Wide Web