

FOR OFFICIAL USE ONLY

**Movement Tracking System (MTS)
Security Features User's Guide (SFUG)**

Version 1.3

25 April 2002

Distribution authorized to the Department of Defense (DoD) and U.S. DoD Contractors only to protect the technical data and operational data from automatic dissemination under the International Exchange Program or by other means, 8 August 2001. Refer other requests for this document to PM GCSS-Army, Attn: MTS, Fort Lee, Virginia 23801-1718.

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

EXECUTIVE SUMMARY	iii
1. Introduction.....	1
1.1. Purpose	1
1.2. Scope	1
1.3. Document Organization	1
2. System security overview.....	3
2.1. Movement Tracking System Security Philosophy	4
2.2. Definition of Terms and Services	5
2.3. The Designated Approving Authority (DAA)	7
2.4. Site Chief/Commander	7
2.5. The MTS Information Assurance Security Officer (IASO)	7
2.6. System Administrator' s Responsibilities	8
2.7. Network Administrator' s Responsibilities	9
2.8. User Security Responsibilities	10
2.9. The MTS User Password Responsibility	11
2.10. Physical Security	12
2.11. Personnel Security	13
2.12. Data Protection	13
2.13. Personnel Security Training and Awareness	13
2.14. Terminal Security	14
2.15. Laptop Computers	15
2.16. Malicious Logic	15
2.17. Security Incident Reporting	16
3. Security Related commands For users.....	17
3.1. Establishing and Ending a Session	18
3.2. Session Initiation	18
3.3. Password Consideration	20
3.4. Password Lifetime	20
3.5. Screen Saver Access	20
3.6. Changing the User Profile	21
3.7. Potential Access Problems And Solutions	21
3.8. Invalid User ID and/or Password	21
3.9. Locking The Workstation	22
3.10. Automatic Locking	22
3.11. Manual Locking	23
3.12. Logging Off The Workstation	23
4. Software Security	24
4.1. Authorized Software	24
4.2. Unauthorized Software	24
4.3. BACKING UP CRITICAL DATA	25

LIST OF FIGURES

Figure 1 DoD User Warning and Consent to Monitoring Banner..... 19
Figure 2 Logon Screen Saver23

EXECUTIVE SUMMARY

This Movement Tracking System (MTS) Security Features User's Guide (SFUG) explains how various system security mechanisms work and how the MTS users may employ some of these mechanisms to consistently and effectively protect their information. "User" in this context refers to a category of people who use the MTS automated information system (AIS) routinely but have no special privileges that would allow them to change the configuration of the system. This guide covers the role and responsibilities of this user category.

This guide provides users with the necessary background and the specific information to use the MTS protection features effectively. Its purpose is threefold: First, it provides the information users need to enter the MTS and start working within its security constraints. Second, it explains the user's role in maintaining the security of the system. Finally, this guide explains what security features are present and how to use the features properly. MTS users are required to consistently and effectively use and protect the MTS and its security-related information as presented in this guide.

1. INTRODUCTION

This Army Movement Tracking System (MTS) Security Features User's Guide (SFUG) is written for the typical user who works with the MTS on a daily basis. Some of the guidance provided herein falls into the broad category of common sense, however, what is common sense for one person, may not be for another so the guidance is included to ensure all MTS users are enlightened. Also, it is very important to remember the security for any system rests with the people who design, manage, administer, and use it so a well designed and managed network with knowledgeable and conscientious users constitutes a very formidable barrier to security breaches and/or network degradation. This SFUG contains information designed to enable individuals at all user levels to better protect the MTS and its supporting infrastructure.

1.1. Purpose

This document is intended to describe the security features that are employed, either actively or passively, by each MTS user on a routine basis. It provides very usable information on the secure configuration and use of the MTS software. It also contains applicable security rules extracted from various policy documents and includes procedures for the MTS and general computer use. In the preparation of this document, policies and procedures from numerous sources were used, including Army Regulation 380-19, Information Systems Security, and other Army regulations and DISA security guidelines (STIGs). This guide applies to all military, civilian and Department of Defense (DoD) contractors who use the MTS.

1.2. Scope

This SFUG describes the MTS user's security responsibilities and provides useful information to assist the user in meeting these responsibilities. When applicable, security features and associated user security responsibilities are described within a subject matter by product. Otherwise, no product distinction is made.

The information in this guide is related, but not limited to, security of the MTS data, MTS user responsibilities, and how each user will perform security-related tasks.

This is not a technical manual. It should be used in conjunction with vendor specific hardware and software documentation in addition to other documentation such as local standard security operating procedures (SSOP), security policy letters, and special MTS Information Assurance Security Officer (IASO) and system administration (SA) guidance and advisories.

1.3. Document Organization

This document has the following sections:

- **INTRODUCTION** Describes the purpose, scope, and organization of the MTS SFUG.
- **SYSTEMS SECURITY OVERVIEW** Gives the reader a high level description of the MTS, describes the MTS security philosophy, lists useful definitions, and briefly identifies the MTS security points of contact and describes the roles of each. It also describes user security responsibilities and gives an overview of the MTS system security.
- **SECURITY RELATED COMMANDS FOR USERS** Describes MTS user procedures for logging on and off the MTS system. It also describes errors that might occur during session initiation and corrective actions for them.
- **SOFTWARE SECURITY** Describes the MTS software security issues to include backing up critical data.

2. SYSTEM SECURITY OVERVIEW

The MTS is the military application of a commercial system that allows movement commanders and control/management personnel to track and communicate with tactical vehicles on a worldwide basis in near-real time. MTS provides text messaging and vehicle tracking capabilities for the U.S. Army that allow a commander to determine where his vehicles are, what their status is, and to communicate with them. The MTS uses a two-way data communications system that provides users in a tactical/non-tactical environment the capability to send and receive GPS provided automatic position reports and text messages anywhere in the world, 24 hours a day. MTS provides the ability to reroute supplies to higher priority needs, avoid identified hazards, and inform operators of unit location changes. The MTS also provides mobile or fixed data communications from single or multiple units. This section provides the background for the overall operation of the security controls in the MTS system so that users will understand the options available to them and the actions a user may take when using individual security-relevant commands.

The system architecture for the MTS consists of User Data Terminals, each with an associated communications terminal, GPS Satellites, Communications Satellites, a commercial Communications Gateway, which contains a communications Hub and a commercial packet switch/server. There are two types of user data terminals:

- A **control terminal**, that provides command functionality for the MTS, and is typically operated from a mobile headquarters, such as a command tent or a parked van
- The **V2 mobile unit** is designated for permanent installation in a vehicle using an installation kit designed for that vehicle

Data to be processed by the MTS has been determined to be sensitive-but-unclassified. In normal operations this data will not be covered by the privacy act. The data will include sensitive combat service support data and highly perishable location data of in transit logistical support vehicles.

Users gain access to the system by providing a terminal log-on at the various data terminals. A local SA locally controls user ids and passwords. Once log-on has been completed, the communications terminal automatically negotiates a system log-on with the packet switch. That log-on is based on a device registration that is controlled by the administrator at the packet switch. Once the logon has been completed, the system automatically begins to send positioning data (if autotrack is selected) and will automatically begin receiving messages addressed to the unit and/or sending messages from the unit to the system.

Encryption if from multiple pre-loaded keys is pre-loaded at the installation. With the option to retain one of these keys for over-the air re-keying (OTAR) from the packet switch if desired or they can be re-loaded locally.

Files residing at the Packet switch are a routing table, a user database, and a message log.

The user database consists of the terminal ID numbers associated with the various terminals operating within the system and their group association with the control terminals. Copies of all the messages and position location data generated by the system are retained in the message log for whatever audits are required.

The Hub also has a routing table.

When the control stations receive a system acknowledgement, they are downloaded from the packet switch an extract of the routing table for their particular group.

Respective Message files, routing tables, and position location files remain active within each terminal as long as power remains applied to the terminal. However, when power is turned off, these files are purged from the active software. The user does however have the capability to save whatever message he wants to retain using the operating system embedded utilities.

Control Stations have the capability to challenge mobile stations that are assigned to their group. If the mobile station does not respond properly to the challenge then it is removed from the system until the challenge is resolved.

2.1. Movement Tracking System Security Philosophy

The MTS relies on the security features incorporated into the operating system at each data terminal to protect the information available at that terminal. Information transmitted through the communications terminal is protected during transmission by encryption with approved type III encryption system. (DES or Triple DES). Each communications terminal is provided access to available network services based on a terminal ID provided by the network systems administrator. This access is automatic once the data terminal comes on-line with the communications terminal. Among the mobile MTS, terminals are associated into groups, organized around a control terminal. Association with a particular group determines which of the MTS mobile terminals provides automatic position location data to the control terminal, and which mobile and control terminals can be addressed with messages. Messaging and position location data can only occur between the MTS terminals in their assigned groups. The SA located at the packet switch/server controls group assignment. Control Stations have the capability to challenge mobile stations assigned to their respective group. If that challenge is not successfully answered, then the challenged station is removed from the network.

Encrypted data (position data or messages) is forwarded through the satellite link to the packet/switch server, where the data is decrypted, stored for auditing functions and then readdressed and re-encrypted for forwarding back through the system to the ultimate addressee. Security among the various user groups is provided by a proprietary "agent" at the packet switch/server. This "agent is also relied upon to secure the data for the separate groups from the Internet connections to the server/packet switch.

2.2. Definition of Terms and Services

The terms and services related to the information contained in this document are specific to the MTS security policy. This section introduces the terms that will be used to describe the security services for which the end-user is responsible. The definitions that follow will assist the end-user in understanding terms used elsewhere in this document:

- Access control: Procedures or mechanisms that restrict use of a computer system to authorized persons and processes only. This includes restrictive mechanisms that permit only authorized users or processes to send or receive messages, and that limit the transmission of messages to those users and processes authorized to receive them
- Accountability: The security mechanisms and processes in place that enable activities to be traced to users and processes that may then be held responsible for those actions
- Audit: The act of gathering usage information on a computer system to allow statistical and performance analysis or to detect and deter AIS penetration or identify system misuse
- Availability: The security mechanisms and processes that ensure resources, services, and data are accessible and usable on demand and in a timely manner by an authorized user or process
- Commercial-off-the-shelf (COTS): Refers to a software or hardware item that has been produced and is available for general purchase. Such items that have been sold and delivered to government or commercial customers must have passed the customer's acceptance testing and must be operating under the customer's control and within the local environment
- Identification: The means by which a user or process provides a claimed identity to a computer system. A user ID is an example of identification
- Site Commander: The person who is assigned the overall security responsibility for that organization
- Password: A unique set of alphanumeric and special characters assigned to or created by a user for use in authenticating the user when logging in to a computer system or application
- Information Assurance Security Officer (IASO): The organizational Information Assurance Security Officer is responsible for system software maintenance and for the organization's adherence to related system security policies and regulations of an information system throughout its life cycle, from design through disposal
- Removable media: Computer media that are easily removed, such as tapes, diskettes, removable hard disk drives, or CD ROMs
- Sensitive-but-Unclassified (SBU): Government-derived and non-government information, of which the loss of could adversely affect national security interests. This information may be withheld from the public under one or more of the

exemptions provided in the Freedom of Information Act (FOIA). Examples of this type of information include computer design data; new processing algorithms; and private company proprietary data

- Security incident: An actual or suspected event or incident, intentional or accidental that places the security of a computer system, or sensitive or classified information, at risk. A security incident could result in a breach of confidentiality, data or system integrity, or system availability
- System Administrator: The individual responsible for the day to day maintenance, securing and monitoring of the information system
- Trojan horse: A computer program containing an apparent or actual useful function that contains additional (hidden) functions that allow unauthorized data collection, falsification or destruction
- User: A person or process accessing the MTS by direct connections (e.g., via terminals) or indirect connections
- Virus: A computer program that embeds itself in other code or software and can replicate itself. Once active, it takes undesired and unexpected actions that can result in either destructive or non-destructive outcomes in the host computer
- Worm: An independent program, similar to a virus, that replicates from machine to machine across network connections often clogging networks and computer systems as it spreads
- MTS Messenger: A software process on the system that provides messaging capability to the control stations and the V2 mobile station
- Tracerlink Tracking: A software process that provides the Global Positioning System (GPS) tracking for the mobile units and provides automatic position reporting through the system
- Tracerlink Mapping: A software process that interfaces the automatic tracking capability with on-board mapping software

The following are services for the MTS:

- Authorized users are created by the system administrator and activated by user logon
- The operating system is an internal function of the laptop software and is activated when power is applied to the laptop
- Loading and configuring the MTS software on an individual laptop system creates the MTS Messenger. Under normal circumstances, the MTS Messenger activates when an authorized user completes the logon progress
- When the MTS software is loaded and configured on a laptop, it creates the Tracerlink Tracing process. Under normal circumstances, Tracerlink tracking is activated when an authorized user completes the logon process in the control stations

and the V2 mobile unit.

2.3. The Designated Approving Authority (DAA)

The DAA for the MTS is the Program Executive Office (PEO), Standard Army Management Information Systems (STAMIS). The DAA formally accepts the level of residual risk for the operation of the MTS and officially declares that adequate safeguards are in place against security threats. Any program-level issues concerning the MTS security are decided by the DAA.

2.4. Site Chief/Commander

The site commander will appoint in writing an IASO for each MTS or group of MT's. The IASO will have overall responsibility for the MTS.

The site commander will also be responsible for establishing a security plan in their command and ensure that the following are accomplished:

- Establish and manage the ISS command program to include defining the ISS personnel structure and directing the appointment.
- Promulgate ISS guidance within each command, to include developing command unique guidance as required
- Ensure that personnel are properly trained

2.5. The MTS Information Assurance Security Officer

For each MTS or groups of MTS, there will be an IASO appointed by the commander or manager of the activity responsible for the MTS. The same IASO may be appointed for multiple MTSSs, particularly in the environment where they are oriented toward the functional user as the operator. The following paragraphs briefly describe the MTS IASO, responsibilities of the position, and the relationship with the MTS user.

There are several positions that have significant roles in network and laptop security but in this respect, the IASO is generally most important to the user. The IASO is the day-to-day network and laptop security person for the MTS. The IASO (or their designated representative) is the first person users should try to contact if they have a laptop-related security problem or issue.

The IASO responsibilities may vary slightly from location to location, but the following are typical, especially for the MTS IASO. The IASO:

- Ensures systems are operated and maintained according to the established procedures and regulations
- Is the focal point for all assigned system security matters
- Provides end-users with system-specific and general awareness security training

- Ensures managers, SA, and users have the appropriate security clearances, authorization, and need-to-know
- Conducts security threat and vulnerability assessments of the MTS
- Monitors system activity, including the identification of the levels and types of data handled by the MTS, the verification of password assignments, and the review of audit trails, outputs, etc., to ensure compliance with the MTS security policies and procedures
- Reports security incidents and technical vulnerabilities to the DAA, the MTS General Manager and the MTS Program Manager
- Maintains access control records and establishes an access control policy in which only authorized personnel can gain access to the system
- Establishes a system for issuing, protecting, and changing system passwords
- Prepares or oversees the preparation of certification and accreditation documentation
- Maintain accreditation documentation and initiate re-certification and re-accreditation when changes affecting security have occurred or when required by AR 380-19, paragraph 3-6
- Implementing appropriate safeguards required by regulations
- Completing an AIS security survey for the MTS and developing the MTS SSOP
- Supports user training, in accordance with the MTS security policies and procedures, and in accordance with the system security requirements specification (SSRS)
- Assists in the development, implementation, and testing of the MTS contingency and incident response plans
- Ensures that only authorized personnel can gain access to the system
- Maintains close liaison with system administrators to promote security at all levels of system operations

2.6. System Administrator' s Responsibilities

The SA is required to keep the MTS operational and the system secure. The following tasks are essential in accomplishing these goals:

- Ensure that the operating system for the MTS is configured properly and that the security features appropriate to the intended level of system operation are properly set. Such settings will be periodically reviewed; such reviews will not involve looking at information or data contained in the files of individual users other than system configuration files
- Periodically check with the operating system manufacturer and the LIWA, in order to keep informed of system security problems and patches as they are developed, and

apply them as appropriate in order to maintain security

- Review file names, length, permissions, and directories. If any of this information leads a SA to suspect that an individual user is misusing the system or engaging in other misconduct, the SA will notify the chain of command
- If a SA suspects an unauthorized user is attempting to access the MTS, the SA is authorized to take the actions necessary to verify and limit the penetration attempt from an unauthorized user. Once verified, the SA will notify, concurrently, the chain of command. The SA may conduct a system backup of appropriate log, history files, and user directories. Once the SA has determined that the anomaly is in fact an unauthorized intrusion, the SA will not in any other manner specifically target, track or attempt to investigate a suspected intruder's activities except as part of a properly authorized investigation

2.7. Network Administrator's Responsibilities

The Network Administrator (NA) operates under similar broad authority and restrictions as the SA. While it is the NA's responsibility to keep the networking infrastructure operational and secure, they operate under the same constitutional and statutory controls as the SA. These restrictions represent a balance between the actions necessary to provide a reliable and secure communications backbone for the MTS, while at the same time ensuring the privacy rights of the users. It is the goal of the NA to ensure the continued operation of the infrastructure which is composed of two major components; the communications medium over which the MTS communications travel; and the network hardware (hubs, switches, etc.,) which make up the physical equipment of the network. The following tasks are critical in achieving the goals of continuity and security:

- Ensure that all hardware and software components of the network infrastructure are properly configured and the security features and controls appropriate to the intended level of system operation are properly set. Such settings will be periodically reviewed to ensure that they are set correctly and have not been modified without the network administrator's knowledge
- Periodically check with the maker of the network components, the LIWA, and/or the DISC4, in order to keep informed of system security problems and patches as they are developed, and apply them as appropriate to maintain the integrity of the network
- Use network management systems to monitor the operational status of the network, and to collect statistics on bandwidth utilization and error rates
- If the NA suspects that an individual user is engaging in any misuse or misconduct, the NA will notify, concurrently, the appropriate Government representative. The NA will not specifically target or track an individual's activities except as part of a properly authorized investigation
- If the NA suspects an unauthorized user is attempting to access a system on the network, the NA will notify, appropriate Government representative. The NA will not

specifically target, track, or attempt to investigate a suspected intruder's activities except as part of a properly authorized investigation

- Use sniffers or network analyzers only as tools in diagnosing network problems

2.8. User Security Responsibilities

Owners, developers, operators and users of the MTS each have a personal responsibility to protect the system's resources. Functional managers have the responsibility to provide appropriate security controls for any information resources entrusted to them. These managers are personally responsible for understanding the sensitivity and criticality of their data and the extent of loss that could occur if their sources are not protected. Managers must ensure that all users of their data and systems are made aware of the practices and procedures used to protect the information resources.

General Responsibilities - All MTS users share certain general responsibilities for information resource protection. The following considerations will guide user actions:

- Treat information as you would any valuable asset. You would not walk away from your desk leaving cash or other valuables unattended. Take the same care to protect information. If you are not sure of the value or sensitivity of the various kinds of information you handle, ask your IASO for guidance
- Observe established policies and procedures. Specific requirements for the protection of information have been established. These requirements may be found in policy manuals, rules, or procedures. Ask your IASO if you are unsure about your own responsibilities for protection of information
- Recognize that you are accountable for your activities on the MTS. After you receive authorization to use the MTS, you become personally responsible and accountable for your activity on the system. Accordingly, your use will be restricted to those functions needed to carry out job responsibilities
- Report any unusual occurrences. Many losses would be avoided if users would report any circumstances that seem unusual or irregular. Warning signals could include such things as unexplainable system activity that you did not perform, data that appears to be of questionable accuracy, and unexpected or incorrect processing results. If you should notice anything of a questionable nature, bring it to your IASO/SA attention

Security and Control Guidelines - Some common-sense protective measures can reduce the risk of loss, damage, or disclosure of information. Following are the most important areas of information systems controls that assure that the system is properly used, resistant to disruptions, and reliable:

- Make certain no one can impersonate you. A password is used to verify the user's identity; this is the key to system security. Do not disclose your password to anyone, or allow anyone to observe your password as you enter it during the log-on process.

Passwords must be at least 8 characters in length and contain at least two numeric characters. If you choose your own password, avoid selecting a password with any personal associations, or one that is very simple or short. The aim is to select a password that would be difficult to guess or derive.

- If your system allows you to change your own password, do so regularly. Passwords on the MTS are required to be changed at least semi-annually. Periodic password changes keep undetected intruders from continuously using the password of a legitimate user
- After you have logged on, the laptop will attribute all activity to your user id. Therefore, never leave your terminal without logging off -- even for a few minutes. Always log off or otherwise inactivate your terminal so no one can perform any activity under your user id when you are away from the area
- Safeguard sensitive information from disclosure to others. Often individuals forget to lock up sensitive reports and laptop media containing sensitive data when they leave their work areas. Information carelessly left on top of desks and in unlocked storage can be casually observed, or deliberately stolen
- While working, be aware of the visibility of data on your laptop or terminal display screen. You may need to eliminate over-the-shoulder viewing
- Label all sensitive diskettes and other laptop media to alert other employees of the need to be especially careful. When no longer needed, sensitive information must be deleted or discarded in such a way that unauthorized individuals cannot recover the data. Printed reports must be finely shredded, while data on magnetic media must be overwritten. Files that are merely deleted are not really erased and can still be recovered
- When data is stored on a hard disk, take steps to keep unauthorized individuals from accessing that data
- Maintain the authorized hardware/software configuration. Computer “viruses” acquired through seemingly useful or innocent software obtained from public access bulletin boards or other sources has affected some organizations; others have been liable for software illegally copied by employees. The installation of unauthorized hardware can cause damage, invalidate warranties, or have other negative consequences. Install only hardware or software that has been acquired through normal acquisition procedures and comply with all software licensing agreement requirements
- Observe the copyright laws for all laptop data

2.9. The MTS User Password Responsibility

Users have the responsibility to memorize and protect their own passwords. Each user who uses the MTS must be aware of and implement the necessary security safeguards as

contained in applicable regulations.

Users will follow the password guidance that has been established in the MTS security policy. The most common technique used to gain unauthorized system access involves password guessing, a form of password cracking. Password cracking is a technique used to secretly gain system access by using another user's account. Users often select weak passwords that can be guessed easily by knowing a little something about the user (e.g., children's names) or passwords susceptible to dictionary attacks (i.e., brute-force guessing of passwords using a dictionary as the source of guesses). The following is a list of suggested guidelines to be used when selecting and protecting passwords:

- Pick a password that is not a word or name but is easy to remember
- Passwords will be at least eight characters long and must contain at least one alpha character (a-z, A-Z) and at least two numeric characters. Non-alphanumeric characters (\$,!,%, etc.) may also be included but at least two numeric characters and one alpha character must be used
- Passwords shall not contain common words, a spouse's or child's name, birth-dates, telephone numbers, or consecutive characters
- Do not keep passwords that may have been delivered with a system
- Do not let anyone know your password
- Do not write passwords down unless they are safeguarded commensurate with their sensitivity or classification level
- Change passwords semi-annually
- If a user believes their password has been compromised, then report the compromise to the MTS IASO immediately of their discovery

2.10. Physical Security

Physical security controls are established to prevent unauthorized access to information in the MTS. The following user guidelines are recommended:

- Protect information against inadvertent access by unauthorized persons
- Use approved containers or areas for storage of information (e.g., printouts, removable media) when unattended
- Double-check the workstation and workspace when leaving it unattended or secured for the day to ensure that all information is appropriately safeguarded
- Secure the V2 computer and transceiver with locking devices or move to secured location when unattended
- Log off laptops or use a password-protected screen lock-out features when leaving work area

Reference the TFM for procedures for investigating suspected unauthorized access attempts.

2.11. Personnel Security

It is a common mistake to think because all users are cleared that there is no need for tight security. Since the MTS operates in the SBU Dedicated Security Mode, all users of the MTS must be cleared, have formal access approval, and a need-to-know for all system data to include the highest level of data processed on the system. Data Protection

The Windows NT operating system contains built-in data protection capabilities which have been configured to provide the necessary amount of access based on user roles and requirements. The file system, registry and audit setting are configured in accordance with the DISA Windows NT Security Checklist. Though the MTS processes no classified or Privacy Act information, the data within the system still must be protected. When a user works with information on the laptop, it is always a good idea to do so in a way so that passers-by or visitors to the workspace cannot view it. Personnel security controls help ensure that only authorized personnel have access to certain types of information. The MTS user is personally responsible for ensuring that only authorized personnel gain access to the data with which the user is working. In addition, the MTS user is responsible for compliance with the guidelines established by the MTS security policy for the protection of the MTS information.

Suggested guidelines are:

- Know the person requesting information and his or her need for the information they are seeking
- Do not give contractors access to any information accessible on them unless first approved through proper channels. Request approval for contractor access through the appropriate contracting officer only when required to satisfy the terms of the contract. The contracting office is responsible for obtaining appropriate nondisclosure agreements and ensuring requirements of the Privacy Act of 1974 are enforced.

2.12. Personnel Security Training and Awareness

Users must be trained before they are given access to the MTS and must receive recurring training thereafter. Listed below are topics each user must understand, most of which are covered in this guide. If a user does not understand any of these topics, it is in their best interest to contact their IASO.

- *Threats, vulnerabilities, and risks associated with the system* - Users must get specific information regarding measures to reduce the threat from malicious software including prohibitions on loading unauthorized software, the need for frequent backup, and the requirement to report abnormal program or system behavior

immediately.

- *Information security objectives (i.e., What is it that needs to be protected?)*
- *Responsibilities and accountability associated with network and computer security*
- *Information accessibility, handling, and storage considerations*
- *Physical and environmental considerations necessary to protect systems*
- *System data and access controls*
- *Emergency and disaster plans*
- *Authorized systems configuration and associated configuration management requirements*

Periodic security training and awareness may include various combinations of the following:

- Self paced or formal instruction
- Security information bulletins
- Security posters
- Training films and tapes
- Computer-aided instruction.

Refer to the MTS Security Awareness Training & Education (SATE) Plan for more information.

2.13. Terminal Security

Unattended terminals logged into the MTS must be safeguarded. On Windows NT 4.0, users must either log out (the preferred method) or use a 32-bit password-protected screen saver when the terminal is left unattended. Regardless of type of operating system in use, users are required to log out of the MTS prior to leaving at the end of the workday.

Windows NT 4.0 is inherently vulnerable. The data on these types of computers plus certain network resources are accessible to anyone with physical access to the machine whether logged in or not. Steps must be in place to deny access to these types of computers; particularly those in common use areas, from unauthorized individuals.

Methods to deny access may include:

- Keeping unauthorized personnel out of workspaces or escorting them while in them
- Keeping selected laptops in locked rooms when unattended
- Using Complementary Metal-Oxide Semiconductor (CMOS) passwords
- Using 3rd party security software

- Lock V2 cradle and secure associated equipment when unattended.

2.14. Laptop Computers

Laptop computers are particularly prone to loss or theft so they must not be left unattended when in use outside the office or during travel unless they are secured in a locked room, locked car, or a locked container such as an airport locker. Laptops must be hand carried (do not check as baggage) when traveling aboard commercial transportation. An individual may be held financially liable if these guidelines are not followed, and they lose their laptop computer through apparent negligence.

Lost or stolen laptops must be reported immediately to the IASO and the unit security manager so they may make an assessment of any damage such as compromised passwords or inadvertent disclosure of other personal data.

2.15. Malicious Logic

Computer systems may be attacked from multiple sources. One of these is called malicious logic, and it may take the form of a computer virus, a worm, a Trojan Horse or various types of “logic bomb” software. For this reason, any imported data package, whether imported electronically or by diskette, must have a virus check performed on it prior to its introduction into the MTS.

There are certain precautions that can be taken to prevent the spread of viruses and related threats. The MTS Security Incident Response Plan must be followed in regard to screening for computer viruses and other malicious logic. The following are some warning signs to look for that may indicate a system is infected:

- Unexplained decrease in PC or workstation memory
- Programs attempting to write-protect media
- Data executable files disappearance
- Delays in program start-up
- Unusual monitor displays and messages
- Unexpected rebooting
- Outgoing electronic mail that the user did not intend to send
- Unexpected changes to volume labels
- Unexplained slow-down in processing time
- Unexpected links to another unauthorized program

2.16. Security Incident Reporting

A computer security incident can result from a computer virus, other malicious code, or system penetration. Without immediate technical expert response, an incident could result in server damage or compromise of business-unit information regardless of its sensitivity. Generally, the user will not take any independent corrective action but will notify the IASO or SA immediately of the incident. The IASO or SA may provide guidance or suggest corrective action depending on the nature of the incident.

3. SECURITY RELATED COMMANDS FOR USERS

The MTS users must be very familiar with the MTS security-related commands and security features and must learn how to use the MTS workstations and terminals with these in mind.

The MTS relies on the security of the local workstation for access to the system. Since each workstation is essentially operating in a stand-alone mode with messaging capability provided through the serial interface by the Comtech Communication Terminal, the only security available is the data terminal log-on process. Once this process is successfully established the communications terminal automatically registers the system with the packet switch.

Through the Windows NT 4.0 operating system, permissions define the types of access allowed for each user and group of users. Windows NT 4.0 maintains these permissions independently for each user. Managing Windows NT 4.0 security, in effect, means managing users and groups, Windows NT 4.0 security is very robust, protecting each shared resource in the system. When a user logs on to a Windows NT 4.0 MTS terminal, the operating system creates a unique access token for that user. This token identifies the user and all the user's access permissions. Each time the user requests access to a shared resource or the user's account runs a program, Windows NT 4.0 checks the token against permission settings and returns a verdict that determines whether the access is allowed.

The Windows NT 4.0 security model is an integral subsystem — security affects the entire operating system. The security subsystem controls access to *objects* (such as a file or printer)

Windows NT 4.0 security provides event auditing and detail logging and lets you monitor the access and use of various resources on the terminal.

The Windows NT 4.0 security model consists of several key components, each of which plays a vital role in the overall security model.

- **Logon Processes (LP)** — accepts logon requests from local users
- **Local Security Authority (LSA)** — ensures that users have permission to access a particular resource on the terminal
- **Security Reference Monitor (SRM)** — ensures that a user or process has permission to access an object by checking the user's security profile. The SRM enforces access validation and any audit policies that have been defined by the LSA

On a Windows NT 4.0 system, users must identify themselves by typing a unique logon name and password before being allowed access to the system. The system uses this identification to track the activities of the user. An authorized SA can audit security-related events and the actions of individual users, which are written to the Event Log where they may be easily reviewed.

3.1. Establishing and Ending a Session

In MTS, each control station system administrator (SA) is charged with the responsibility of administrating user accounts and passwords for his or her particular group. The system is delivered with one, generic, built-in, user account. The account also has a pre-defined password. Because MTS operates in a dedicated security mode, one in which all users must have approval and a need to know system specific data, all authorized users have permission to use one generic Windows NT user account and corresponding password. An SA may enforce a more stringent user account policy as required.

The MTS provides the user with a multi-step process, which allows the user to access all authorized resources, on the basis of a single user authentication process that is performed when the user initially accesses the system.

3.2. Session Initiation

The Windows NT 4.0 logon process is mandatory for initiating a session. The logon is a multi-step process. The user will enter the UserID and password. The password is hashed and sent to the Local Security Authority (LSA). The LSAs makes a call to the authentication package and compares the hash to the hash stored in the local SAM database. The LSA creates an access token using the information returned from the authentication package and the NT Explorer shell with the user's access token attached.

Logging on to the MTS establishes user identification and authenticates the user, which is a necessary component of the MTS security. Once a user receives the logon dialog, he or she is required to enter his or her userid and password. Both username and password are looked up in the MTS Security Account Manager (SAM) database. If there is a successful match, the system will give the user a unique security token that contains user account information and establishes a session. This security token, called an "access token," is used to identify the user for the duration of the session (until they log off the system). The access token is transparent to the user and contains a user's security identifier (SID), group id's, and user right. Each token contains the following information:

- User's Security Identified
- User privileges
- Owner SID (Assigned to any objects created during the session)
- Default Access Control List (ACL) (Assigned to any object created by the user)

After a successful login, the "DoD user warning and consent to monitoring" notice will be displayed (refer to Figure 1 immediately below.) followed by a login window. To

continue on the MTS, user must consent to monitoring. Lack of consent will forfeit access to the network resources.

“USE OF THIS OR ANY OTHER DOD INTERNET COMPUTER SYSTEM CONSTITUTES A CONSENT TO MONITORING AT ALL TIMES”. This is a Department of Defense (DOD) interest computer system. All DOD interest computer systems and related equipment are intended for the communication, transmission, processing, and storage of official U. S. Government or other authorized information only. All DOD interest computer systems are subject to monitoring at all times to ensure proper functioning of equipment and systems including security devices and systems, to prevent unauthorized use and violations of statutes and security regulations, to deter criminal activity, and for other similar purposes. Any user of a DOD interest computer system should be aware that any INFORMATION PLACED IN THE SYSTEM IS SUBJECT TO MONITORING AND IS NOT SUBJECT TO ANY expectation of privacy. If monitoring of this or any other DOD interest computer system reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring of this or any other DOD interest computer system reveals violations of security regulations or unauthorized use, employees who Violate security regulations or make unauthorized use of DOD interest computer systems are subject to appropriate disciplinary action. “USE OF THIS OR ANY OTHER DOD INTEREST COMPUTER SYSTEM CONSTITUTES A CONSENT TO MONITORING AT ALL TIMES”

Figure 1 DoD User Warning and Consent to Monitoring Banner

3.3. Password Consideration

User identification and password systems support the minimum requirements of accountability, access control, least privilege, and data integrity. The IASO or designated representative is responsible for managing, and control of all passwords. On the MTS, the SA will be responsible for managing the change of passwords.

Passwords which validate access to SBU data on the MTS will be protected as For Official Use Only (FOUO) Per Army Regulation 25-55.

After creation, passwords will be handled and stored at the level of the most sensitive data contained in the system. Knowledge of passwords will be limited to a minimum number of persons. Passwords will be issued if the user has a confirmed authorization to access the system

At the time of password issuance, individual users will be briefed on the following:

- Password classification and exclusiveness
- Measures to safeguard classified and unclassified passwords;
- Prohibitions against disclosure to unauthorized personnel, even though they may be assigned to the same project and hold identical clearances; and
- The requirement to inform an IASO or designated representative immediately of password disclosure or misuse or other potentially dangerous practices.

3.4. Password Lifetime

A password will be issued only once and will be retired when the time limit, 180-days, has expired. The SA is responsible for managing and changing passwords as they expire.

Passwords on the MTS will expire 180 days after the laptop is initially started at the factory for all users. CAUTION: On the SCI manufactured V2 laptop, there is no CAPS Lock indicator light). Password history is maintained, so a SA cannot reuse the same passwords. The operating system remembers the last ten (10) passwords used for each user. Three consecutive incorrect password attempts within 30 minutes will lock out a user until the SA re-enables the user.

Passwords will be inhibited, overprinted, or otherwise protected from unauthorized observation on terminals and video displays.

3.5. Screen Saver Access

Although not required, Windows NT 4.0 allows the use of a screensaver that will control user access to the workstation when left idle for 3-5 minutes. The screensaver will utilize the MTS user accounts within Windows NT 4.0 and will require a valid userid and password to re-obtain access to the MTS.

Upon the system being in locked mode, only the current user or a user with administrative privileges will be able to regain access. The screensaver will be set to activate upon

being idle for 3 -5 minutes.

3.6. Changing the User Profile

The “profile” file defines the user login environment in accordance with a set of access permissions established by the MTS SA. These files are executed automatically by the system whenever a user logs in. Whenever a change to the system environment becomes necessary, a user must request the change through the SA in order for a change to be made for their “profile” files in their home directory. Any changes to the way a login is executed require a change to the profile and must be approved based on a need-to-know. The changes become effective the next time the user logs in.

3.7. Potential Access Problems And Solutions

The identification and authentication (I&A) security requirements built into the MTS require that the user enter a user ID and password before access to the system is granted. Based on I&A information and the configuration of the user profile, the user will be provided with the appropriate access rights and privileges to access specific data.

During normal operations, the user may encounter access errors. Some causes and corrective actions or explanations for the access problems are provided in the following subparagraphs.

3.8. Invalid User ID and/or Password

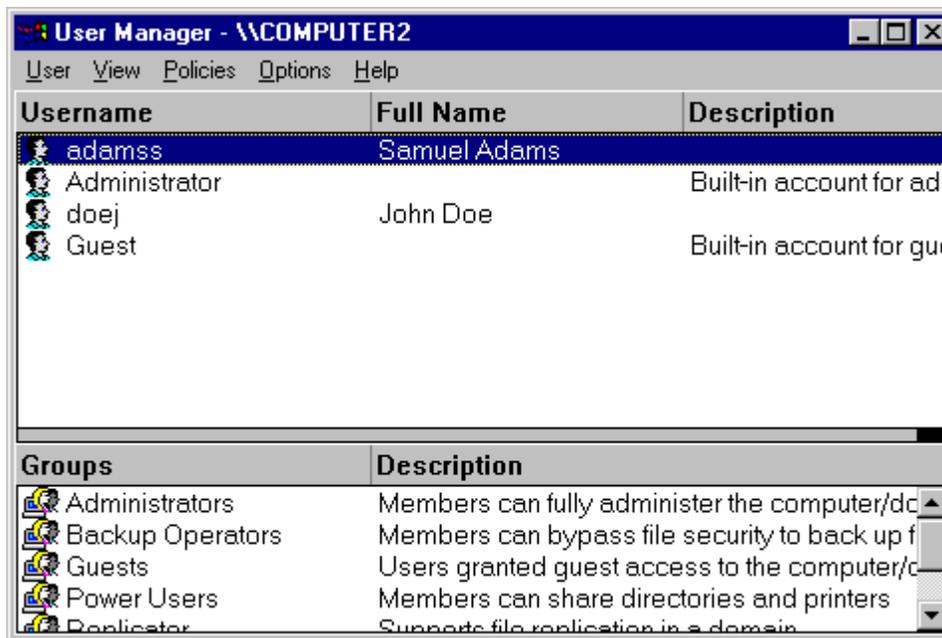
If the user ID or password is invalid for the MTS system, the message “Incorrect login”, Try again” appears, and the prompt reappears. When the SA activates the system lockout feature, the system will respond to the number of consecutively failed user login attempts. Generally, three unsuccessful login attempts using the same user ID will trigger system lockout and disable any further login attempts at the terminal until the terminal can be unlocked (reset) by the SA.

3.9. Locking The Workstation

When leaving their workstation for any length of time, users must either log off or lock the workstation in order to protect the workstation and the user's data from passers-by who can take advantage of the open session. MTS security policy requires users to utilize the terminal lock feature to prevent unauthorized access to the system and sensitive data. Prior to leaving a terminal unattended, the user must activate the terminal lock feature. Once executed, the monitor will display a blank screen and prevent anyone from viewing sensitive data. After the terminal lock feature is activated, future access to the terminal is granted only after entry of a valid User ID and password.

3.10. Automatic Locking

Although it is not a requirement, the user can configure the workstation to automatically lock itself after a set period of time by selecting a screen saver that has the Password Protect option. To configure the Workstation to lock itself with a screensaver after a



specified period of inactivity, perform the following:

- Double-click on “**My Computer**”
- Double-click on “**Control Panel**” and then double-click on the “**Display**” icon to bring up the window shown in the figure below

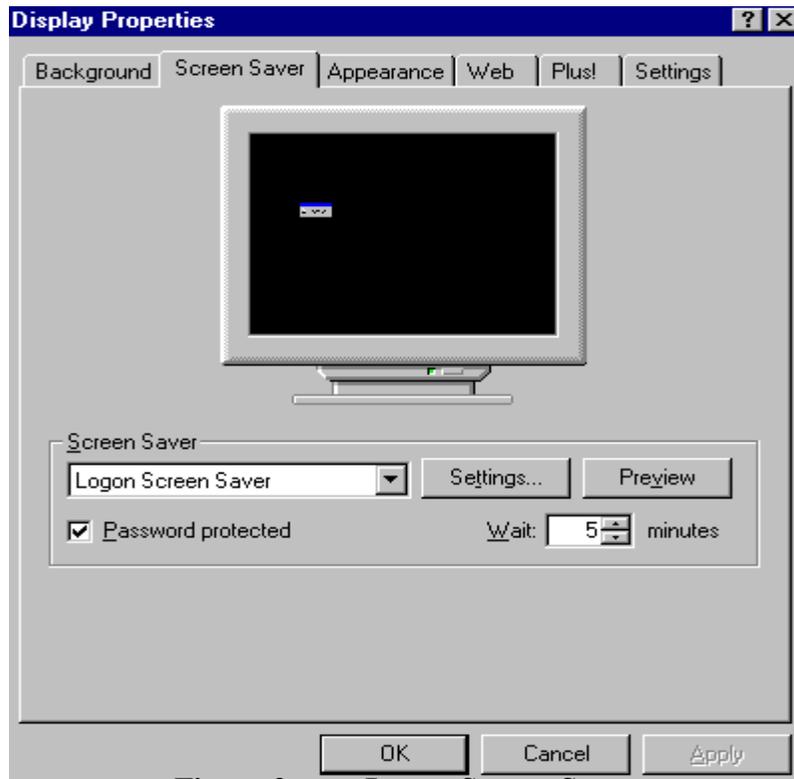


Figure 2 Logon Screen Saver

- Click on the Screen Saver tab
- Select the 32-bit screen saver that displays a “Logon Screen Saver”
- Click the “Password protected” checkbox to enable the lock out feature and then set the amount of time before it is invoked. The amount of time should be set at 3 to 5 minutes.

NOTE: The password that will be used when this screen saver is invoked is the one that was given to the user when their MTS account was created on this workstation.

- Click on **OK**

3.11. Manual Locking

To manually lock the workstation, press **CTRL+ALT+DEL** and then choose the “Lock Workstation” button in the Windows NT Security dialog box.

To unlock the workstation, press **CTRL+ALT+DEL** and type your password into the “Workstation Locked” dialog box.

3.12. Logging Off The Workstation

Logging off the system at the end of the workday or before a long absence is mandatory.

- To logoff, click on the **Start button**
- Click **shutdown** and then click **OK**

4. SOFTWARE SECURITY

MTS software must be controlled to protect the MTS from compromise, subversion, or unauthorized manipulation.

4.1. Authorized Software

Only software that is authorized by the MTS system administrator and is required to accomplish the mission should be loaded. Authorized mission critical software includes:

- Windows NT 4.0, SP6a, accessories, and hot fixes
- MTS Messenger 2.06
- Tracerlink Pro 2.0.11
- McAfee Virus Scan 4.0.5
- Adobe Acrobat 5.0
- Inside Out Networks Drivers 1.26
- NIMA Maps

The MTS IASO must approve all software a user wishes to load on his or her system. Generally, the IASO will approve the following types of software:

- Standard COTS software from major software vendors that has been properly procured and is required to accomplish the MTS mission
- Software provided by the U.S. Army or other DoD agency

The system manufacturer retains all application media. If a failure occurs, it will be resolved at the component level as a standard maintenance action. If spare systems are on-site, they will be implemented. The local SA will not be required to maintain and secure software media. Printed data should be treated as a sensitive item and be secured appropriately.

All authorized software, to include data generated during the use and execution, is critical to the mission of the MTS system. Data sensitivity is, at the minimum, equal to that of the system.

4.2. Unauthorized Software

A user must not download programs and/or file attachments from untrusted sources over the Internet or through e-mail whether they know the sender or not. The following unauthorized software will not be downloaded:

- Any sexually oriented material of any type, or other types of entertainment software is expressly forbidden. This type of software is a prime source of viruses and/or Trojan

horse, particularly when downloaded from the Internet.

- Do not violate software copyrights. Maintain documentation to prove that the software has been properly procured. If shareware is utilized, ensure the proper fees have been paid to the vendor.
- Remove trial versions of software that are not purchased at the end of the trial period. Be particularly aware of trial versions of software that are downloaded from the Internet. Software in this category includes, but is not limited to WINZIP, DISKEEPER, and various Symantec products. Purchase or remove the software at the end of the trial period.
- Intrusive software includes software that is specifically designed as packet analyzers with the purpose of capturing system passwords or to provide unauthorized remote control of a PC or server. Examples of intrusive software programs include, but are not limited to, Spy, Crack, Satan, Sniffer, Back Orifice, NetZero and Netbus.
- Any software that may impact network or common user system (such as e-mail) performance.
- Evaluation copies of software from major software vendors
- Software commonly referred to as shareware or freeware. For the purposes of this instruction, this is software produced by individuals or small software vendors for fee distribution or a small fee per copy.
- Locally written or compiled software.

4.3. BACKING UP CRITICAL DATA

Operational data (i.e. messages, position data, etc.) is perishable and is not saved to file upon exit of the MTS application; therefore, backups are not required. If an application error were to occur, the system would be repaired via a standard maintenance action. MTS provides spare quantities that may be issued as needed. System data may be printed for later use, but must be appropriately safeguarded.

4.4. Protecting System From Viruses

Every laptop connected to the MTS must have McAfee Anti-Virus software loaded. The SA will be responsible for ensuring that control stations are scanned and have updated definition files on a weekly basis and that mobile units are scanned and updated upon insertion of new software. The following guidance will help protect the MTS from viruses at the user level:

- Scan diskettes, compact disc, downloaded files, and zip disks prior to uploading files on an MTS.
- Only official business should be conducted on the MTS. Most viruses are received from unofficial files or programs that users load on their computers.

Refer to the MTS TFM for more information.

APPENDIX A: LIST OF ACRONYMS

AR	Army Regulation
CD ROM	Compact Disk Read Only Memory
COTS	Commercial-Off-The-Shelf
CMOS	Complementary Metal-Oxide Semiconductor
DAA	Designated Approving Authority
DoD	Department of Defense
DoDIIS	DoD Intelligence Information System
DISC4	Director of Information Systems, Command, Control, Communications and Computers
FOIA	Freedom of Information Act
I&A	Identification and Authentication
IAW	In Accordance With
ID	Identification
IS	Information System
IASO	Information Assurance Security Officer
IT	Information Technology
LIWA	Land Information Warfare Activity
NT	Network
PC	Personal Computer
PM	Program Manager
SA	System Administrator
SATE	Security Awareness Training and Education
SBU	Sensitive –But Unclassified
SFUG	Security Features User's Guide
SSRS	System Security Requirements Specification
SSOP	Security Standard Operating Procedure
TDY	Temporary Duty
TFM	Trusted Facility Manual
User ID	User Identification

APPENDIX B:REFERENCES

DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP)," December 30, 1997.

Army Regulation, 380-19, Information System Security, 27 February 1998.