FEASIBILITY OF DEVELOPING A SECURE GATEWAY

FINAL

Prepared for:

Directorate of Information Science and Technology

Defense Technical Information Center
Cameron Station
Alexandria, Virginia 22304-6145

April 23, 1992

Contract Number: MDA903-90-D-0022

Task Order: 20

Prepared by:

George A. Buchanan
David Scheidt

IIT Research Institute
4600 Forbes Boulevard
Suite 200
Lanham, Maryland 20706

FEASIBILITY OF DEVELOPING A SECURE GATEWAY

DRAFT

REPORT 3 OF 3

Prepared for:

Directorate of Information Science and Technology

Defense Technical Information Center
Cameron Station
Alexandria, VA 22304-6145

10 April 1992

Contract Number: MDA903-90-D-0022

Task Order: 20

Prepared by:

George A. Buchanan
David Scheidt

IIT Research Institute
4600 Forbes Boulevard
Lanham, MD 20706

EXECUTIVE SUMMARY

1.0 INTRODUCTION

The DoD Gateway Information System (DGIS) effort began in the early 1980s to provide a one-stop user-friendly access to many federal and commercial databases. The present effort is to determine the feasibility of developing an intelligent, secure gateway to classified databases, such as the Defense RDT&E Online System (DROLS), and the Air Force's CIRC database, in addition to unclassified databases, such as those already available with DGIS. A secure gateway consists (conceptually) of three major components: a secure operating system, telecommunications, and application software.

This report presents the results of a study of the feasibility of developing a secure gateway. Three types of characteristics required for the secure gateway are discussed: functional, security, and technical characteristics. To provide assurance of the technical feasibility of a secure gateway, trusted computing base (TCB) components are mapped to secure gateway features. Then various configuration options for developing a secure gateway are presented. System solutions for developing a secure gateway are then offered, which are followed by estimated component costs for a secure gateway. The cost of three configurations for implementing the secure gateway are offered as system solutions. Last, the certification process for a secure gateway is presented. The certification process of a secure gateway must be determined by the gateway's designated approving authority, i.e., Defense Logistics Agency (DLA) and/or National Security Agency/National Computer Security Center (NSA/NCSC).

2.0 SECURITY ISSUES

For a DGIS-like gateway to operate in a multilevel secure environment, certain issues must be addressed. A fundamental issue is the certification of such a "secure gateway", which requires satisfying applicable security regulations. It is desirable that the operating system used in the secure gateway satisfy Class B2 criteria, as specified in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC). This is because Class B2 satisfies the risk analysis according to the National Computer Security Center's (NCSC) publication, Computer Security Requirements (CSC-STD-003-85). In particular, Class B2 allows both classified and unclassified users to simultaneously access the secure gateway. This evaluation assumes that the secure gateway is a closed environment, an open environment would require Class B3. The aforementioned publication (on page 12) states: "Where a system processes classified or compartmented data and some users do not have at least a Confidential clearance, or when there are more than two types of compartmented information being processed, at least a class B2 system is required." In contrast to Division C, Division

B trusted computer systems can be certified to operate in multilevel secure environments. Class B2 features required for the secure gateway, which are lacking in Class B1 systems, include the use of: subject sensitivity labels, device labels, trusted communication paths, covert channel analysis, trusted facility management, and configuration management.

3.0 TECHNOLOGICAL ISSUES

Currently being evaluated by NCSC at the B3 level is the secure operating system, Trusted Mach. This operating system promises to become an industry standard. Trusted Mach has a POSIX interface, which is UNIX-like; and will be portable to a variety of platforms. Trusted Mach systems, though, may not be commercially available for another two years.

In this report, application software is considered to be software other than vendor-supplied operating system software, and must be developed or adapted for use in the secure gateway. Application software includes two basic categories; the user interface and communication interfaces. For a secure gateway, the user interface software includes the menu system that the user sees, and the underlying software that provides functionality for the menu options. Communication interfaces for a secure gateway include device drivers and additional software, which are required for the secure gateway to communicate with external systems, such as user systems and database systems. Application software developed for the gateway must have a trusted interface with the underlying secure operating system. This trusted interface must include "software hooks" required by the operating system's security kernel, which serves as the "security filter" for all interactions with the gateway. The "software hooks" are the means for transferring essential security information between the application software and the secure operating system. These "software hooks" are discussed further in the body of this report. As shown in the following paragraph from the TCSEC, application software not residing within the TCB boundary does not require certification.

The TCSEC preface has the following general discussion on the use of its criteria.

> "The criteria provide a basis for the evaluation of effectiveness of security controls built into automatic data processing system products. The criteria were developed with three objectives in mind: (a) to provide guidance to manufacturers as to what to build into their new, widely-available trusted commercial products in order to satisfy trust requirements for sensitive applications and as a standard for DoD evaluation thereof; (b) to provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information; and (c) to provide

a basis for specifying security requirements in acquisition specifications. Two types of requirements are delineated for secure processing: (a) specific security feature requirements and (b) assurance requirements. Some of the latter requirements enable evaluation personnel to determine if the required features are present and functioning as intended. The scope of these criteria is to be applied to the set of components comprising a trusted system, and is not necessarily to be applied to each system component individually. Hence, some components of a system may be completely untrusted, while others may be individually evaluated to a lower or higher evaluation class than the trusted product considered as a whole system. In trusted products at the high end of the range, the strength of the reference monitor is such that most of the system components can be completely untrusted. Though the criteria are intended to be application-independent, the specific security feature requirements may have to be interpreted when applying the criteria to specific systems with their own functional requirements, applications or special environments (e.g., communications processors, process control computers, and embedded systems in general). The underlying assurance requirements can be applied across the entire spectrum of ADP system or application processing environments without special interpretation."

Secure gateway software that lies within the secure gateway's trusted computing base (TCB) must be certified by the DLA and/or NSA/NCSC. Once certified, this software is considered to be trusted. Secure gateway software that lies outside of the secure gateway's TCB does not require DLA and/or NSA/NCSC certification. This software is considered to be untrusted.

A primary goal of each secure gateway configuration considered is to allow both classified and unclassified users to have convenient full access to all of the databases mediated by the secure gateway, that the respective users are authorized to access. The user interface should be independent of the type of secure gateway option used. That is a user will not be able to recognize how the secure gateway is configured. Because the secure gateway will automatically distinguish between classified and unclassified sessions, users accessing the secure gateway in an unclassified sessions will not require secure communication equipment, e.g., STUs, nor will unclassified users require clearances. The secure gateway will provide users with automatic logins to databases that are allowed for the user's clearance and the current classification of the user's session. The secure gateway will regulate access to the results of classified queries. For example, the secure gateway will allow an authorized (cleared) user to query classified databases during unclassified sessions, but not classified or otherwise sensitive information can be viewed during an unclassified session.

The security of classified communications is the joint responsibility of both the remote sites and the secure gateway. No classified transmissions must be allowed through the insecure communication channels of unclassified sessions. For example, the secure gateway and DROLS will regulate access to classified and otherwise sensitive information on DROLS. DROLS is a multi-level secure system which contains databases that include both classified and unclassified data. Access to DROLS data is in part regulated by the use of communication ports that have been designated for use in either classified or unclassified transmissions. These two types of ports are shown in the figures in the discussions of the various possible secure gateway configurations.

4.0 CONCLUSION

This study concludes that a Class B2 secure gateway can be developed with existing technology. Of the options reviewed, a secure gateway based on a multilevel secure local area network could provide the required performance at the best cost of "commercial-off-the-shelf" (COTS) products. The essential technologies for this option are Trusted Information System's (TIS) Trusted XENIX, Verdix's VSLAN, and Ethernet connections. Trusted XENIX is a certified Class B2 trusted (UNIX) operating system, that can be used on personal computers based on the Intel 80386 or 80486 processors. VSLAN is a certified Class B2 secure local area network that can be used with Trusted XENIX to provide a secure gateway with the required performance.

If the secure gateway's development were delayed until Trusted Mach is available, this secure operating system could serve to provide a more affordable standardized trusted environment than currently available certified operating systems. Also, Trusted Mach is anticipated to be certified higher than Class B2.

Crucial to implementing the secure gateway is the demonstration of application software that has the required "hooks" to the underlying secure operating system. The rest of the gateway consists of hardware and software technology that already exists or will become available in the foreseeable future. The incorporation of the remote access communication channels in the secure gateway should also be straightforward.

TABLE OF CONTENTS

FIGURES

1.0 INTRODUCTION

The secure gateway discussed in this report is intended to provide to authorized users the same functionality as the Defense Technical Information Center's (DTIC) DoD Gateway Information System (DGIS). This functionality will extend to multilevel classified databases. Classified use of the secure gateway will subject users to additional access procedures. Unclassified use of the secure gateway will appear to be the same as DGIS from the user's perspective. This perceived similarity in classified sessions vs. unclassified sessions is achieved by keeping nearly all classified operations of the secure gateway from the user's view. The primary user-related differences between classified and unclassified sessions result from the requirement that the user must be identified and be authorized to perform classified operations, e.g., additional passwords may be required. Also the secure gateway will automatically recognize the classification of a session.

1.1 BACKGROUND

The secure gateway is to provide authorized users with access to classified databases from a central point, while preventing such access by unauthorized users. It will allow both classified and unclassified authorized users to have access to unclassified databases. The secure gateway is intended to operate much like the existing DGIS, except that security features must be added to the hardware, operating system, and certain application software.

In this report, application software is considered to be software other than vendor-supplied operating system software, and must be developed or adapted for use in the secure gateway. Application software includes two basic categories: the user interface and communication interfaces. For a secure gateway, the user interface software includes the menu system that the user sees, and the underlying software that provides functionality for the menu options. Communication interfaces for a secure gateway include device drivers and additional software, which are required for the secure gateway to communicate with external systems, such as user systems and database systems. Application software developed for the gateway must have a trusted interface with the underlying secure operating system. This trusted interface must include "software hooks" required by the operating system's security kernel, which serves as the "security filter" for all interactions with the gateway. The "software hooks" are the means for transferring essential security information between the application software and the secure operating system. As indicated in the

Department of Defense Trusted Computer System Evaluation Criteria[1] (TCSEC) preface, only that application software that lies within the secure gateway's Trusted Computer Base (TCB) boundary is considered to be trusted application software and requires certification. The "look and feel" of DGIS should be retained in the secure gateway, thus allowing users to use the new secure gateway with minimal training. Much of the existing DGIS software may be suitable for use in the secure gateway, either totally, or partially by adapting the software to satisfy modified requirements. To provide these capabilities, the secure gateway must exhibit various functional, security, and technical characteristics.

The feasibility of developing a secure gateway for DTIC is determined by various factors. These factors include the satisfaction of regulations, the availability of technology, the cost of products and services, and the certification process. The satisfaction of regulations is based on the secure gateway having various security characteristics. The cost of the secure gateway is based on both cost of products and services and development schedule. Before the gateway can begin service, the secure gateway's designating approving authority (Defense Logistics Agency and/or National Security Agency/National Computer Security Center) must certify it. The Defense Logistics Agency (DLA) provides the computer security requirements for DTIC. The National Security Agency's (NSA) National Computer Security Center (NCSC) sets United States Department of Defense computer security standards.

The following two subsections provide background information on secure operating systems and their relationship to trusted application software.

1.1.1 Secure Operating System

The security features provided by the operating system for the secure gateway is fundamentally important to the security of the gateway and the data that it handles. The secure operating system must satisfy at least all essential Class B2 TCSEC criteria, i.e., those associated with labeling. When the system security administrator registers a user, device, port, etc., the TCB assigns sensitivity labels to the respective subject, object, or device. User registration information on the various external databases, e.g., DROLS, need not be duplicated in the secure gateway by the gateway's system security administrator. Critical to developing application software for the secure gateway (e.g., the user interface and communication interfaces) is the interface between

---

[1] U.S. Department of Defense (DoD), Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200.28-STD, December 1985.

the application software and the secure operating system. The interface must allow the passing of security-related information between application software and the secure operating system. This security-related information includes user IDs, passwords; and data, device, and port sensitivity labels. The transfer of this information is required to ensure the security and integrity of classified or otherwise sensitive information handled by the secure gateway. For example, the sensitivity label of a communication port must be provided to the secure operating system with each communication between the operating system and the port.

1.1.2 Trusted Software Applications Using Secure Operating Systems

Trusted computer software can be modeled with a tiered, four ring structure. The lower rings have the highest privileges while the highest rings have the lowest privileges. (Refer to FIGURE 1.1.) Ring zero, the lowest ring, is the operating system security kernel and operates across the entire computer regardless of classification of data. Ring zero is the most secure portion of the software. Users do not have direct access to ring zero. Ring one consists of the input/output (I/O) and system service routines. Like ring zero, users do not have direct access to ring one and the ring is highly secure. Ring two is divided into two portions of software, application programs written by programmers which access ring one, and "commercial-off-the-shelf" (COTS) software which has been certified. This certified COTS software, in combination with the software in rings zero and one, comprise all of the trusted software. The majority of the software developed for the secure gateway will reside in ring three. Ring three contains low privilege application routines.

All application routines, and data associated with them, which are contained in ring three, are compartmentalized by the security kernel and the trusted software. A user with a classification level of "unclassified" must only be permitted access to the software and databases contained in the unclassified portion of the system. Likewise, classified users can only access that information contained in the classified portion of the system. The result of this approach is that applications developed for ring three are secure, because the TCB software will not allow software in this ring to commit a security violation.

An unfortunate side effect of developing the secure gateway on ring three is that, for some commercial secure operating systems, classified users must not be permitted access to unclassified databases while they operate at a classified level. This problem could be overcome by either of two methods. The user can change his level to be unclassified during his access to unclassified databases, or the secure operating system could be modified to allow for access to lower levels of classification. Changing the

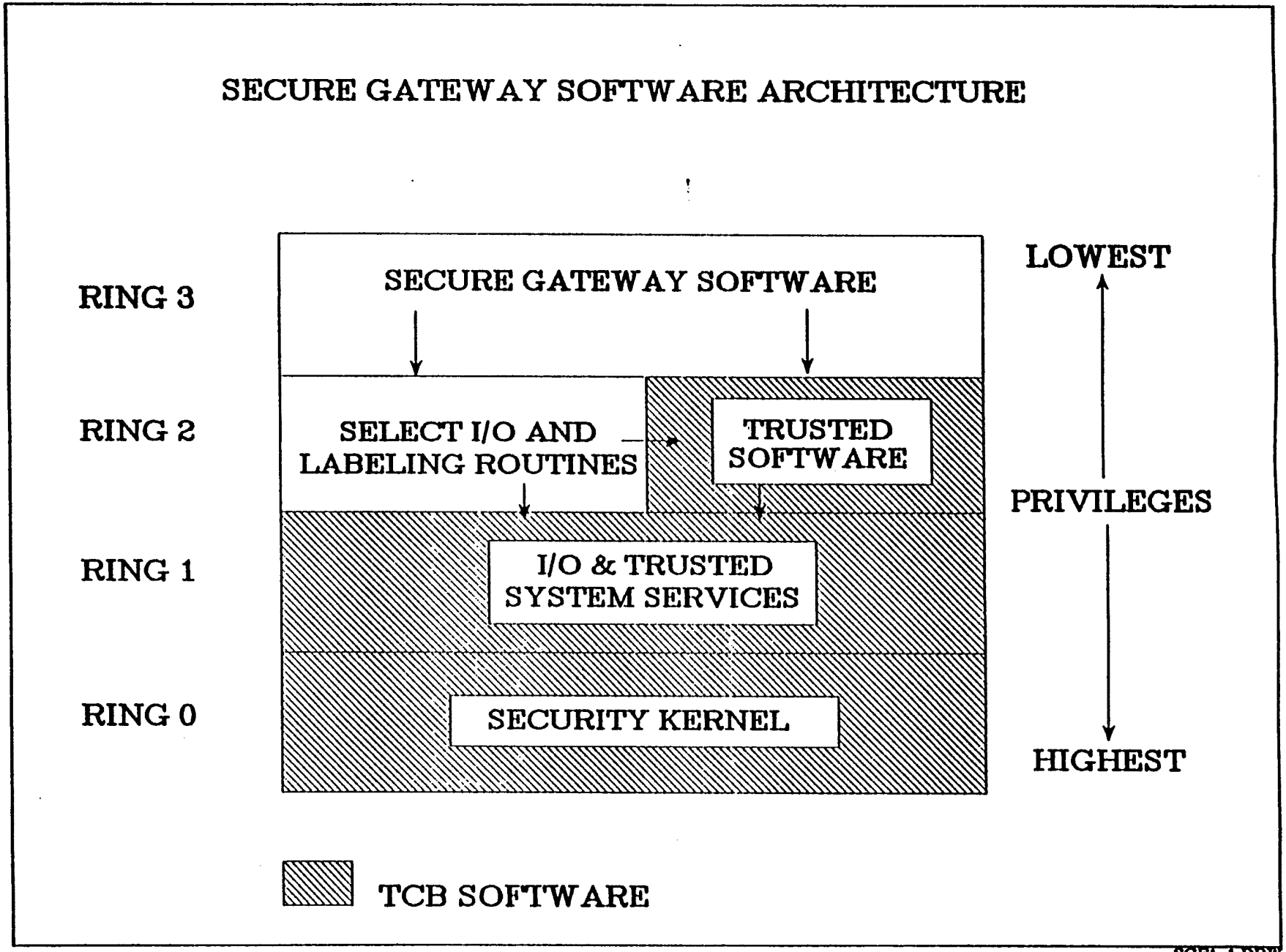


FIGURE 1.1 SECURE GATEWAY SOFTWARE ARCHITECTURE

user's classification level can be done by the user at an operating system prompt for at least one of the systems, i.e., HFSI's XTS-200/STOP. Changing classification level in a more automated fashion may require modifying the secure operating system because any program or shell that executes the classification change cannot itself be contained in ring three. The cost in time and effort required to make such modifications to a COTS system and then to get the COTS system recertified may prove to be unacceptable. Such modifications of a COTS secure operating system would require coordination with the vendor of the system. At least one COTS system, HFSI's XTS-200/STOP, is capable of allowing access to lower classification levels managed by the secure operating system.

1.2 PURPOSE

This document is a feasibility study for developing a secure gateway. Its conclusions are based on the research presented in two earlier reports: Security Regulations Relevant to Developing and Using a Secure Gateway[2] (SGSR), and Evaluation of Technologies for Developing a Secure Gateway[3] (SGT). The first report examined security regulations and mapped them to the requirements for developing the secure gateway. The second report examined security technologies that are applicable to the secure gateway. For more detailed information on security regulations and technologies, refer to these two earlier reports.

The remainder of this document examines how the aforementioned factors that determine the feasibility of developing a secure gateway can be addressed. The following six sections assess the impact of these factors: required characteristics, technology, configuration options, system solutions, cost, and certification.

---

[2] Buchanan, George, and Steven Goldstein, Security Regulations Relevant to Developing and Using a Secure Gateway, IIT Research Institute, February 1992.

[3] Buchanan, George, and Steven Goldstein, Evaluation of Current Technologies for Developing a Secure Gateway, IIT Research Institute, February 1992.

2.0 REQUIRED CHARACTERISTICS OF THE SECURE GATEWAY

This section discusses characteristics required by the secure gateway for it to provide secure DGIS-like operations. These characteristics are grouped into functional, security, and technical characteristics.

2.1 FUNCTIONAL CHARACTERISTICS

The secure gateway must provide DGIS-like functionality to authorized users. This functionality must support the DGIS features stated in the DGIS Users' Guide[4] (Page 1-1). This quote is provided as a baseline to confirm the secure gateway's functionality.

> "DGIS offers two modes: menu mode and command mode. Menu mode offers all of the DGIS options in a logical progression of menus. Each DGIS option is also a command and can be used at any point within DGIS. DGIS also offers several utility features that are not presented on the menus. These commands are known as interrupt commands. Using either menu mode or command mode in conjunction with the interrupt commands, DGIS users can take advantage of the following features:
>
> 1. Connecting to other computer systems (using either search interfaces or native mode).
> 2. Downloading bibliographic citations from other computer systems.
> 3. Examining the Directory of Online Resources.
> 4. Running several processes simultaneously.
> 5. Analyzing and reformatting downloaded citations (post-processing).
> 6. Sending and receiving electronic mail.
> 7. Carrying out file operations."

The secure gateway must provide features that correspond to the seven DGIS features listed above and some additional features. Corresponding DGIS-like features are included below with the additional qualification that the secure gateway's DGIS-like features must handle classified or otherwise sensitive information

---

[4] Defense Technical Information Center (DTIC), Gateway User Support and Training Office, DGIS Users' Guide, (DoD Gateway Information System), August 1989.

as well as unclassified information. The previously stated DGIS features are stated again to show that they are accounted for in the secure gateway and to help clarify the mapping of functional features to technologies in Section 3.0.

A. Provide connections to other classified and unclassified systems (using either search interfaces or native mode).

B. Access unclassified databases using SearchMAESTRO.

C. Allow downloading of records from other classified and unclassified systems, e.g., downloading bibliographic citations from other computer systems.

D. Allow examination of the Directory of Online Resources. Restricting access to this unclassified sensitive information may be required.

E. Allow post-processing of classified and unclassified citations; e.g., analyzing and reformatting the citations, and merging these citations into a single file.

F. Provide classified and unclassified electronic mail (E-Mail), "Talking", and "Linking" to exchange information between authorized users. Such information exchanges will be restricted by the secure gateway to authorized users.

G. Text-editing capabilities.

H. Provide general utilities, e.g., performing file operations on classified and unclassified information.

I. Allow several simultaneous classified and unclassified processes.

J. Provide for automatic login and logout, including handling of passwords to remote systems. (Security of passwords is discussed below in Section 2.2, Security Characteristics, item B.)

2.2 SECURITY CHARACTERISTICS

Applicable security regulations for the secure gateway have been identified in the first report[2] (SGSR) mentioned above. This section, using various perspectives, proposes means of satisfying these regulations. Classified sessions must appear to users to be essentially the same as unclassified sessions. A few security-related differences must appear in the initial classified session menus vs. unclassified sessions menus. Otherwise, the software

underlying classified sessions must satisfy security requirements that are not applicable to software for unclassified sessions.

The secure gateway must have the following security measures to satisfy applicable security regulations. The labeling mechanism referred to below is the sensitivity labeling mechanism defined in the TCSEC for implementing mandatory access controls (MAC).

A. The secure gateway must operate in a multilevel secure (MLS) environment. This MLS operation requires that the secure gateway must ensure the security and integrity of the operating system and network. Classified use of the secure gateway must subject users to additional access procedures. Unclassified use of the secure gateway must appear the same as DGIS from the user's perspective. The secure gateway must recognize the classification of a session. Any file that contains multilevel classified citations will be assigned by the secure gateway the highest classification of any citations within the file.

B. Trusted application software, such as that used in trusted parts of the user interface and communication interfaces, must have "software hooks" to the secure operating system and secure network(s).

C. Secure access to multilevel classified databases. DGIS functionality of the secure gateway must extend to multilevel classified databases. Accesses to classified databases must be either through multilevel secure means or be considered to be at the security level of the highest classified data being accessed (e.g., "citation high").

D. Securely manage classified or otherwise sensitive information by regulating access to compartmentalized multilevel classified data.

E. Communication with the secure gateway must be via trusted communication paths through the secure gateway's trusted communication interfaces. Trusted communication paths connect classified users through the secure gateway to remote classified databases. The transmission of classified data via communication channels must be labeled. Communication ports must be labeled. Users must not be allowed access to system software other than for executions.

F. File management operations, such as, create, write, read, copy, and delete, must be regulated to ensure the security and integrity of accesses to and modifications of files.

G. Human-readable output must be labeled, as specified in the TCSEC. Thus, classified or otherwise sensitive information must be labeled at the field, citation, and/or file level; depending on the availability of the classification of the information in the originating database.

H. An audit trail of accesses and modifications to classified or otherwise sensitive information must be maintained. An audit trail of remote accesses is very important for security and charging.

I. Access to information on the existence of classified resources in the Directory of Resources must be regulated. Though the resources may be classified, the directory is considered to be unclassified/sensitive.

J. The security policy of the secure gateway must be enforced by a system security administrator.

K. Physical Security, Contingency Plans, and Personnel Security must be provided for the secure gateway.

2.2.1 Software Hooks Between Application Software and Secure Operating System

The secure operating system must be able to recognize and to track the presence, or use, of all interactions with classified or otherwise sensitive information handled by the secure gateway. Application software for the secure gateway (e.g., the user interface and communication interfaces) must have "software hooks" to the underlying secure operating system. The secure operating system is fundamentally responsible for the security of all interactions with the secure gateway. The following "software hooks" are required for the interface between application software and the secure operating system.

A. User IDs and Passwords (The input of passwords must be passed to the secure operating system. Passwords must be managed by secure means, e.g., user passwords must be encrypted so that even the system administrator and the system security administrator cannot know the passwords.

B. Device IDs and Sensitivity Labels

C. Port IDs and Sensitivity Labels

D. Classification of Data from Databases (with Sensitivity Labels) will be assumed to have the same classification that the data has in its originating databases.

E. Classification of Files (with Sensitivity Labels) - A merged file becomes classified according to the highest classification level of data within the file.

F. Directories and Subdirectories (with Sensitivity Labels)

G. Allowable Input/Output Operations (with Sensitivity Labels)

H. Remote Terminals (with Sensitivity Labels)

I. Communication Channels (with Protocols and Sensitivity Labels)

These "hooks" must be provided by the secure operating system. Users and devices in the above list are automatically tagged by the TCB with sensitivity labels when the system security administrator registers their identification and authorization for access to the secure gateway. Subsequently, the TCB's security kernel associates all registered users and devices with their sensitivity labels. Each sensitivity label contains information on the authorized security level of its corresponding user or device. The security level includes both authorized secrecy levels and categories, and integrity levels and categories. The categories refer to compartmentalized information. After the authorizing association, all interactions with the secure gateway by all such registered users and devices are monitored by the TCB.

2.3 TECHNICAL CHARACTERISTICS

Platform:

The secure gateway's platform must provide the following.

A. The secure gateway' performance must be responsive to users' needs so as to promote rather than hinder users performing their tasks. For example, users should experience no more than a one second delay response to entering a key stroke. If processing takes longer than this key stroke delay, then the user should be promptly notified that the processing is being performed.

B. The secure gateway must provide adequate storage (RAM, cache, and hard disk) for all users. Storage must be provided to handle downloaded files, post-processing files, E-Mail files, system software and application software, profiles, etc.

C. The secure gateway must provide a convenient means for the system administrator and system security administrator to interact with the secure gateway (e.g., a monitor, a keyboard, and perhaps a mouse).

Communications:

The secure gateway must have the following features to provide adequate secure communications:

A. Enough ports for the maximum number of simultaneous users.

B. Encryption devices (e.g., STU-IIIs and/or KGs).

C. Transmission/Reception devices (e.g., STU-IIIs and Data Service Units/Channel Service Units (DSUs/CSUs)).

D. Essential Connections/Cabling (e.g., RS-232C or Ethernet).

3.0 TECHNOLOGIES

This section examines various technologies with respect to required characteristics of the secure gateway discussed above in Section 2. The first subsection discusses the applicability of secure gateway technologies to providing the required characteristics of the secure gateway. This discussion addresses issues raised in Section 2.2. The second subsection provides a mapping of required secure gateway characteristics to technologies, which provides a basis for determining the technological feasibility of implementing the secure gateway.

3.1 APPLICABILITY OF SECURE GATEWAY TECHNOLOGY

This section discusses resolutions of the issues raised in Section 2.2. In these resolutions, secure gateway mechanisms are identified that will provide the means of handling these issues. First, as an introduction, certain technical terms are defined.

The following terms are used below. The term "Trusted Computer System" (TCS) refers to the combination of trusted computer hardware and the secure operating system (SOS). The term "Trusted Communication Path" (TCP) refers to a communication path that has mechanisms for ensuring the security and integrity of data transmitted between a TCB and external devices or systems. These mechanisms may include a combination of KGs and modem/DSU with dedicated telephone lines, or (multilevel secure) STU-IIIs with dial-up or dedicated telephone lines. A STU-III is a "Secure Telephone Unit", which contains both encryption/decryption and modem capabilities. Modems are used for transmitting and receiving telecommunication information, e.g., via telephone lines. The term "Trusted User Interface" (TUI) refers to that part of the user interface that lies within the secure gateway's TCB boundary. The term "Trusted Network" (TN) is used in the context of the TNI[5].

The secure gateway will operate in a multilevel secure environment. The secure gateway's TCB will protect classified and otherwise sensitive information in this environment. The TCB mechanisms that will provide this protection are the SOS, TCP, TUI, and TN.

DGIS functionality of the secure gateway will extend to multilevel classified databases. Accesses to classified databases will be either through multilevel secure means or be considered to be at the security level of the highest classified data being accessed (e.g., "citation high"). For a user to gain access to a remote database system, the secure gateway will send the user's password

---

[5] National Computer Security Center, Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria (TNI) (NCSC-TG-005 Version-1), 21 July 1987.

for the remote system to the remote system. This transmission of the user's password may be initiated either by the user or automatically by the secure gateway, depending on the mode of database query used by the user. The security of accesses to classified databases will be ensured by the secure gateway's TCB mechanisms: SOS and TCP.

Users will not be allowed to have direct access to databases. That is, access to databases can not be done without the mediation of the secure gateway, which regulates access to the databases. This access issue may be resolved by segmenting classification levels of data and software used to access classified data, as can be done by commercially available secure operating systems.

Multilevel classified citations will be securely managed by the secure gateway. This classified citation issue may be resolved by segmenting classification levels of data and software used to access classified data, as can be done by commercially available secure operating systems. The mingling of multilevel classified data (e.g., multilevel secure searching, and post processing) will be regulated by the secure gateway's TCB mechanisms: SOS and TUI. Files containing citations having different classifications will be labeled at the classification of the citation having the highest classification. The classification of each citation will be recorded in such files.

Communication with the secure gateway will be via trusted communication paths through the secure gateway's trusted communication interfaces. Trusted communication paths connect classified users through the secure gateway to remote classified databases. This communication issue may be resolved by segmenting classification levels of data and software used to access classified data, as can be done by commercially available secure operating systems in combination with trusted communication paths. The transmission of classified data via communication channels will be labeled. Communication ports will be labeled. Users will not be allowed access to system software other than for executions.

Access to classified E-Mail, "Talking", and "Linking" will be regulated by the secure gateway's TCB. Trusted E-Mail is provided on some secure operating systems in combination with trusted communication paths. Full implementation of "Talking" and "Linking" may require the creation of additional application software, which will probably require coordination with the secure operating system's vendor.

Direct access to classified data by an otherwise authorized classified user from an unclassified terminal (e.g., at home) will be prevented by the secure gateway (i.e., avoiding the secure gateway's regulation of access to resources). That is, only those operations that do not reveal classified information (e.g., querying databases) will be allowed. Classified files resulting

from such queries will be saved, but the user will not be allowed to access such files during an unclassified session. To access these files the authorized user must be in a classified session.

Communication Channel Related Issues	Satisfying TCB mechanism(s)
E-Mail	SOS, TCP, and TUI
"Talking"	SOS, TCP, and TUI
"Linking"	SOS, TCP, and TUI
Trusted Paths	SOS, encryption and transmission devices
Emission Security	Tempest facility and encryption devices

To help provide file protection, memory and disk storage will be partitioned according to user authorization and data classification. This storage partitioning issue may be resolved by segmenting classification levels of data and software used to access classified data, as can be done by commercially available secure operating systems.

Commercially available secure operating systems maintain audit trails of accesses and modifications to classified or otherwise sensitive information. The audit trail can also be used to determine charging for system usage, e.g., by remote accesses.

Access to information on the existence of classified resources in the Directory of Resources will be regulated. Though resources may be classified, the directory is considered to be unclassified but sensitive. If revealing the existence of the resources in the directory is determined to be unacceptable, then the secure gateway will regulate access to this sensitive information on a need-to-know basis. This access can be regulated using discretionary access controls (DAC) to recognize user authorization and mandatory access controls (MAC) to recognize the security level of the session. The secure gateway's secure operating system will regulate access to information identified in the Directory of Resources.

The system security administrator will use the security features of the secure gateway's secure operating system to enforce the secure gateway's security policy.

The requirements for the security policy for the secure gateway can at least be partially satisfied by the existing security policy for

Defense RDT&E Online System (DROLS). Also, the secure gateway's security policy must account for the additional security demands of items such as files and possibly mixed unlabeled data.

3.2 MAPPING OF SECURE GATEWAY CHARACTERISTICS TO TECHNOLOGIES

This section examines various technologies with respect to required characteristics of the secure gateway discussed above in Section 2. Each technology is identified as applicable to satisfying the characteristics from Section 2, the TCSEC, and the NSA's System Security Policy for the Security Enhanced DoD Gateway Information System[6], December 20, 1991 (Section 4.0 Security Policy) that are most relevant to the technology. The items listed below for the NSA security policy refer to subsections in Section 4.0 of the security policy. A copy of this NSA security policy is in Appendix B. A given technology is considered "applicable" if the functionality of the technology is pertinant to the secure gateway characteristic. "Failure" of a given technology to completely satisfy a given secure gateway characteristic means that the technology is not adequate to support this required characteristic. Some technologies may be both "applicable" and "failures"; in these instances the technology does address the secure gateway characteristic, but in a manner which does not satisfy the requirements.

1.0 Secure Operating Systems (Classes B1, B2, B3):

Three of the secure operating systems evaluated in the earlier technology evaluation report[3] (SGT) were AT&T's System V/MLS, Trusted Information Systems's Trusted XENIX, and HFSI's XTS-200/STOP. These three secure operating systems have been certified by the NSA/NCSC at the TCSEC's Class B1, B2, and B3 respectively. Although System V/MLS is certified at Class B1, it does satisfy Class B2 Mandatory Access Controls, but it lacks required Class B2 assurance. Similarly, Trusted XENIX is certified at Class B2; and it satisfies two Class B3 criteria, Discretionary Access Controls and Trusted Path. Even so, Trusted XENIX fails to provide complete Class B3 assurance. In contrast to the other two secure operating systems, XTS-200 provides trusted recovery, which is a Class B3 criteria. The greater the security provided in an operating system the more demands are placed on the performance of the underlying hardware platform. Typically, a few DGIS-like functions are not fully provided in COTS secure operating systems, e.g., "Talking" and "Linking". For the secure gateway to have these functions, the addition of

---

[6] National Security Agency, System Security Policy for the DoD Gateway Information System, October 28, 1991.

trusted application software may be required for their full implementation. Another function required of the secure gateway's MLS operating system will be to allow a user to (automatically) access databases classified at levels below the user's current session classification level.

1.1 Class B1:

Class B1 secure operating systems can satisfy most of the functional requirements and some of security requirements of a secure gateway. The functional requirements satisfied include accessing databases and post-processing of citations. The security requirements satisfied include secure file operations, identification, authentication, and auditing of system use.

Class B1 is applicable to satisfying:

2.1:	A, B, C, D, E, F, G, H, I
2.2:	A, B, C, D, E, F, G, H, I, J
2.2.1:	A, D, E, F
Security Policy (4.x):	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13

Class B1 does not provide adequate mandatory access controls (MAC), e.g., those listed below under TCSEC. These MAC capabilities are required in the secure gateway's operating system to ensure the security and integrity of classified or otherwise sensitive information managed by the secure gateway. The absence of these MAC capabilities in the secure operating system can be compensated by incorporating the capabilities in trusted application software. This fix would cause the secure gateway to be more difficult to certify, than having the MAC capabilities integrated into the secure operating system.

Class B1 does not satisfy:

TCSEC:	Subject Sensitivity Labels
	Device Labels
	Trusted Path
	Trusted Facility Management
	Trusted Recovery
2.2.1:	B, C, G, H, I

1.2 Class B2:

Class B2 secure operating systems can satisfy the functional and security requirements of a secure gateway. The functional requirements satisfied include E-Mail and general utilities. The security requirements satisfied include required mandatory access controls and trusted paths lacking in a Class B1

system.

Class B2 is applicable to satisfying:

2.1:	A, B, C, D, E, F, G, H, I
2.2:	A, B, C, D, E, F, G, H, I, J
2.2.1:	A, B, C, D, E, F, G, H, I
Security Policy (4.x):	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13

Class B2 lacks the desirable TCSEC operational assurance provided by trusted recovery. Trusted recovery provides procedures and/or mechanisms to assure that, after a system failure or other discontinuity, recovery without a protection compromise can be obtained.

Class B2 does not satisfy:
TCSEC: Trusted Recovery

1.3 Class B3:

Class B3 secure operating systems can satisfy the functional and security requirements of a secure gateway. The functional requirements satisfied include text editing and "Talking". The security requirements satisfied include all mandatory access controls provided in Class B2 plus the desirable TCSEC operational assurance provided by trusted recovery. Trusted Mach is anticipated to be certified by the NSA/NCSC at the TCSEC's Class B3. Vendors are promising to offer Trusted Mach systems in about two years (1993 - 1994 time frame).

Class B3 is applicable to satisfying:

2.1:	A, B, C, D, E, F, G, H, I
2.2:	A, B, C, D, E, F, G, H, I, J
2.2.1:	A, B, C, D, E, F, G, H, I
Security Policy (4.x):	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13

2.0 Application Code:

Application code will have to be developed to fully provide the desired secure gateway functionality. Certain functions, e.g., specialized communication port guards, "Talking", and "Linking", are not adequately implemented in COTS systems.

All application code that lies within the secure gateway's TCB boundary must be certified by the DLA and/or NSA/NCSC as trusted software. The secure gateway's requirements specification will state the boundary of the secure gateway's TCB, as defined by the DLA and/or NSA/NCSC. This TCB

definition will serve to identify the application software required to be certified. DLA and/or NSA/NCSC certification is complicated by the amount of code that must be certified. The more difficult the certification the more expensive will be developing the trusted software. The expense involves additional development time to assure the reliability of the trusted software and the subsequent financial cost of the software development.

The extent of trusted application software required for the secure gateway will depend on the extent that classified data will be passed between application software and the underlying secure operating system. As stated earlier, the boundary of the secure gateway's TCB will be defined by the DLA and/or NSA/NCSC. This TCB definition will determine the extent of the application software required to be certified. The larger the trusted application code, the more difficult it will be to get the code certified by the DLA and/or NSA/NCSC.

"Software hooks" will be implemented with trusted software that provide connections within the secure gateway's TCB between the SOS, TCP, and TUI. These "hooks" will be the only means of transferring classified or otherwise sensitive information between the trusted application code and the secure operating system and secure network(s). For example, the input of passwords will be passed to the secure operating system. Passwords will be managed by secure means, e.g., user passwords must be encrypted so that even the system administrator and the system security administrator cannot know the passwords.

2.1 Small Trusted Application Code:

The introduction of trusted application software should be limited as much as possible to minimize DLA and/or NSA/NCSC certification requirements. The smaller the trusted application code, the easier it will be to get the code certified by the DLA and/or NSA/NCSC.

An example of small trusted application code may be that created to implement specialized trusted communication port guard software. This guard software is intended to protect the secure gateway against unauthorized external access through the secure gateway's communication ports, yet allow the secure gateway to access external systems, e.g., those of remote users and remote databases.

Small trusted application code is applicable to satisfying:

Communication interfacing (e.g., guard software)

2.1: A, B, C, J

2.2: A, B, C, D, E

2.2.1: A, B, C, D, E, F, G, H, I
Security Policy (4.x): 2, 3, 4, 5, 6, 7, 9, 11, 12, 13

2.2 Extensive Trusted Application Code:

The development of extensive trusted application code may be required for the full implementation of certain secure gateway functions. The extent of trusted application software will depend on the security requirements of various features of the secure gateway and the extent to which these features are satisfied by the selected COTS secure operating system. Therefore, trusted application code for the same feature may range from small to extensive, depending on the secure operating system used. If the trusted application code for these functions proves to be extensive, then the software development for these functions would be correspondingly expensive in time and effort. This expense would be required for the code be certified by the DLA and/or NSA/NCSC.

Extensive trusted application code is applicable to satisfying:

Interfacing with the secure operating system
(e.g., MLS searching and MLS post processing)
2.1: A, C, E, F
2.2: A, B, C, D, E
2.2.1: A, B, C, D, E, F, G, H, I
Security Policy (4.x): 2, 3, 4, 5, 6, 7, 9, 11, 12, 13

2.3 Untrusted Application Code:

Untrusted application code will not lie within the secure gateway's TCB and thus will not require certification will be determined by the DLA and/or NSA/NCSC. Untrusted application code is code that either has no interaction with classified or otherwise sensitive data, or has its access to classified or otherwise sensitive data controlled by ring two. This untrusted application code is shown in FIGURE 1.1 as the lowest privileged software in ring three and partly in ring two. Untrusted application code provide those secure gateway functions that are not required to be certified as secure, e.g., the menu system.

Untrusted application code is applicable to satisfying:

Most of User Interface (e.g., Menus)
2.1: B, D, F, G, H, I, J

Untrusted application code is not suitable for:

Interfacing with the secure operating system

3.0 Secure Local Area Network:

A secure local area network can be used to enhance the capabilities of a set of secure computers. Secure local area networks (LAN) provide a means of securely connecting various separate secure computer systems into a larger secure arrangement that can significantly increase the available resources for each computer system. Also a secure LAN allows efficient transfer of information between the secure computer systems within the secure LAN. The file server in a secure LAN can be a centralized secure file manager for all secure computers within the LAN.

A secure local area network, used with a trusted operating system on various nodes of the LAN, is applicable to satisfying:

2.1:	A, B, C, D, E, F, G, H, I, J
2.2:	A, B, C, E
2.2.1:	A, B, C, D, E, F, G, H, I
2.3:	Communications: A, B, C, D
Security Policy (4.x):	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13

4.0 Facility Security:

Facility security is required for providing the secure gateway with physical, emission, and personal security. A secure facility is required for the secure gateway to operate in a secure environment. The secure gateway's TCB alone can not provide physical, emission, and personal security. These additional security requirements can be provided by a secure facility such as that for DTIC's DROLS.

Facility security is applicable to satisfying:

TCSEC:	Trusted Facility Management
2.2:	K
Security Policy (4.x):	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13

5.0 Platform (Hardware):

The secure gateway will reside on an adequate hardware platform that can provide the required system performance. This includes such hardware as adequate cabling for communications and sufficient disk storage for file management.

An adequate secure gateway hardware platform is applicable to satisfying:

2.1:	A, B, C, D, E, F, G, H, I, J

2.2: E, F
2.3: Platform: A, B, C

6.0 Communications (Hardware):

The secure gateway will have adequate hardware communication connections and devices that can provide the required telecommunication performance. Unencyrpted communications must be transmitted within a trusted facility. The security of accesses to classified databases will be ensured by the secure gateway's TCB mechanisms: SOS and TCP.

6.1 RS-232C Connections:

RS-232C is suitable for making basic connections between the secure gateway components and between the secure gateway and certain external systems.

RS-232C connections are applicable to satisfying:
A point-to-point connection inherently provides more assurance of the security of a communication path than can a network connection, e.g., using Ethernet. The enhanced assurance of a point-to-point connection, vs. that of a network connection, is because the former only has a single communication path, where as the latter allows multiple communication paths from a point.
2.1: A, B, C, F
2.2: E
2.3: Communications: A, B, C, D

RS-232C connections are not suitable for networking in local area networks or wide area networks, because the connections within and among these networks are typically designed for Ethernet rather than RS-232C.

RS-232C Connections are not suitable for:
Networking

6.2 Ethernet Connections:

Ethernet is primarily intended for use in making connections within and among networks.

Ethernet connections are applicable to satisfying:
Secure network connections, e.g., a secure LAN such as Verdix's VSLAN.
2.1: A, B, C, F, J
2.2: E
2.3: Communications: A, B, C, D

6.3 Encryption Devices (STU-IIIs and KGs):

Encryption devices such as STU-IIIs (Secure Telephone Unit) and KGs are fundamental to implementing trusted communication paths. These devices encode data to be transmitted and decode data received that may be intercepted while being transmitted via insecure means, e.g., standard telephone lines. Encryption devices, including current MLS STU-IIIs, lack the ability to swap classification levels during a session. Automated MLS functionality in the secure gateway will be able to offset this disadvantage.

Encryption devices are applicable to satisfying:

2.2: A, C, F, J
2.3: Communications: A, B, C, D
Security Policy (4.x): 2, 3, 9, 11

6.4 Telecommunication Devices (Modems and DSUs/CSUs):

Telecommunication devices such as modems and DSUs/CSUs are required for implementing communication between remote systems, e.g., the secure gateway and remote users, and the secure gateway and remote database systems. These devices convert data into serial bit patterns for telecommunication transmissions, e.g., via telephone lines. Modems modulate transmitted signals and demodulate received signals. Modems use analog transmissions. DSUs/CSUs use digital transmissions.

Telecommunication devices are applicable to satisfying:

2.1: A, B, C, F, J
2.2: C, E
2.3: Communications: A, B, C, D

4.0 CONFIGURATION OPTIONS

This section discusses five basic secure gateway connectivity designs. Sections 4.1 and 4.2 discuss the first two options, which are two designs that provide direct connections between the secure gateway and DGIS. The distinction between the first two designs is that connections are made in the first design using Ethernet whereas the second design uses RS-232C to make connections. Section 4.3 discusses the third option, which, in contrast to the first two options, has a design that combines DGIS and the secure gateway in a single multilevel secure computer arrangement. Section 4.4 discusses a multilevel secure (MLS) terminal access controller configuration based on a Gemini Computer. Section 4.5 discusses a MLS local area network (LAN) version of the secure gateway, based on Verdix's VSLAN and TIS's Trusted XENIX.

Of the five options considered, at least in the short term, Option 5 is better able to provide the functional, security, and technical characteristics (discussed in Section 2.0) of the secure gateway. Option 5 is also the most cost effective option to achieve the required performance of the secure gateway. In addition, as the need arises, Option 5, provides a convenient mechanism for expanding the secure gateway, i.e., by adding more personal computers with Trusted XENIX to the MLS LAN. Options 1 or 3, using Trusted Xenix, could serve as a prototype that could evolve into Option 5.

A primary goal of each of these configurations is to allow both classified and unclassified users to have convenient full access to all of the databases mediated by the secure gateway, that the respective users are authorized to access. Thus, the intent of each of the options proposed below is to provide all of the fuctional, security, and technical characteristics discussed in Section 2.0. The user interface should be independent of the type of secure gateway option used. That is a user will not be able to recognize how the secure gateway is configured. Because the secure gateway will automatically distinguish between classified and unclassified sessions, users accessing the secure gateway in unclassified sessions will not require secure communication equipment, e.g., STUs, nor will unclassified users require clearances. The secure gateway will provide users with automatic logins to databases that are allowed for the user's clearance and the current classification of the user's session. The secure gateway will regulate access to the results of classified queries. For example, the secure gateway will allow an authorized (cleared) user to query classified databases during unclassified sessions, but no classified or otherwise sensitive information can be viewed during an unclassified session.

The security of classified communications is the responsibility of both the remote sites and the secure gateway. No classified transmissions must be allowed through the insecure communication

channels of unclassified sessions. For example, the secure gateway and DROLS will regulate access to classified and otherwise sensitive information on DROLS. DROLS is a multi-level secure system containing databases which include both classified and unclassified data. Access to DROLS data is in part regulated by the use of communication ports that have been designated for use in either classified or unclassified transmissions. These two types of ports are shown in the figures below that show various possible secure gateway configurations.

Currently being evaluated by NSA/NCSC at the B3 level is the secure operating system, Trusted Mach. This operating system promises to become an industry standard. Trusted Mach has a POSIX interface, which is UNIX-like; and will be portable to a variety of platforms. Trusted Mach systems, though, may not be commercially available for another two years. Such a Class B3 system would satisfy the requirements for a secure gateway based on Options 1, 2, 3 and 5 to be certifiable by the NSA/NCSC. Trusted Xenix, which is only Class B2, would also satisfy these requirements although Trusted Mach would improve the security in Options 1, 2, 3, and 5. Neither Trusted Mach or Trusted Xenix is applicable to Option 4, because this option uses a proprietary secure operating system from Gemini.

The evaluations of the security requirements for the five secure gateway options were based on the assumption that the secure gateway would operate in a closed security environment. A closed environment requires that the application developers and software maintenance personnel have clearances at a secret level, and that the configuration control provides sufficient assurance against the introduction of malicious logic. If the operating environment of the secure gateway is to be an open rather closed environment then the security requirements will be more stringent for these five options.

4.1 OPTION 1 - TWO GATEWAYS CONNECTED WITH ETHERNET

Option 1, as shown in FIGURE 4.1, provides a means of regulating access to classified and unclassified databases. It consists of a central computer, which contains the secure gateway software, and connections to users and databases. Encryption and telecommunication equipment are used for securely transferring classified information over these connections. If the user is authorized and his equipment is certified for classified communication, then the user may access the secure gateway in either a classified or an unclassified session. These communication options are shown in the FIGURE 4.1 below. To minimize the threat of disclosure of classified information on the secure gateway to users who are in a DGIS session, which is always unclassified, the secure gateway is isolated from DGIS. This separation of DGIS and the secure gateway provides more security and integrity of classified or otherwise sensitive information in the secure gateway than if DGIS were integrated with the secure

gateway into a single MLS system (Option 3 below).

Ethernet is an efficient data transfer medium. Though Ethernet can be used for point-to-point connections, it is intended for use in networks (e.g., LANs). "The Ethernet specification involves only the physical and data-link layers of LAN. Computer-specific hardware (Ethernet controllers) and software (Ethernet driver routines) are required to implement the remaining layers of network control. At the physical level, an Ethernet LAN . . . [is connected] with a coaxial cable of bandwidth 10 million bits/s forming the backbone of the network. Up to 1024 nodes can be connected to the network and their maximum separation is limited to 2.8km."[7] (page 502)

A risk analysis of Option 1, based on the publication, Computer Security Requirements - - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, results in the requirement that this configuration must be certified to at least a TCSEC Class B2. This analysis assumes that the secure gateway is in a closed security environment and its security operating mode is controlled and multilevel. As stated in the NSA/NCSC computer security requirements publication[8] (page 3), a closed security environment is "an environment in which both of the following conditions hold true:

1. Application developers (including maintainers) have sufficient clearances and authorizations to provide acceptable presumption that they have not introduced malicious logic. Sufficient clearance is defined as follows: where the maximum classification of the data to be processed is Confidential or less, developers are cleared and authorized to the same levels as the most sensitive data; where the maximum classification of the data to be processed is Secret or above, developers have at least a Secret clearance.

2. Configuration control provides sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications."

On page 4, the NSA/NCSC computer security requirements publication[8] states that a controlled security mode is "the mode of operation that is a type of multilevel security mode in which a more limited

---

[7] Hayes, John P., Computer Architecture and Organization, 2nd Edition. New York: McGraw-Hill, 1988.

[8] DoD Computer Security Center (DoDCSC), Computer Security Requirements - - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments (CSC-STD-003-85), 25 June 1985.

amount of trust is placed in the hardware/software base of the system, with resultant restrictions on the classification levels and clearance levels that may be supported."

The use of Trusted Xenix with this option satisifies most of the required functional, security, and technical characteristics (discussed in Section 2.0), including trusted E-Mail. The primary deficiencies of this configuration are that Trusted Xenix must run on an IBM AT compatible personal computer, which has an insufficient number of communication ports, and that Trusted Xenix lacks trusted "talking" and trusted "linking", without the addition of trusted application code.

The ability to access DGIS directly will give secure gateways the ability to utilize RAM and file storage on the DGIS computer for storage of unclassified data. This will allow the secure gateway user (in unclassified mode) the capability to utilize the DGIS talking and linking facilities. These capabilities are only possible in options 1 and 2. In addition, some of the software required to access unclassified databases may be executed remotely from the DGIS computer reducing the storage, cpu and security requirements for the secure gateway.

Use of the following available technologies can be used to satisfy the required functional, security, and technical characteristics for this option of the secure gateway. This is not the only suitable set of available technologies.

1. Secure Operating System (Class B2): Trusted XENIX, or
   Secure Operating System (Class B3): XTS-200/STOP

2. Application Code:
   Application code must be custom made for the secure gateway. The extent of trusted application code required for a given secure gateway function will depend on the COTS secure operating system of the secure gateway. This trusted application code will be primarily be associated with interfacing the secure operating system with the user interface and and communication interfaces, e.g., for the implementation of trusted "talking" and trusted "linking."

3. Facility Security: Similar to that for DTIC's DROLS

4. Platform (hardware):
   80386/80486 Personal Computer with an AT bus, or
   Dual Processor DPS 6000

5. Communications (Hardware):
   1. Connections: Ethernet

2. Encryption Devices:
   To remote user: AT&T STU-III Secure Data Device, Model 1900

   To remote databases: AT&T STU-III Secure Data Device, Model 1900

3. Telecommunication Devices: (Modems)
   To remote user: AT&T STU-III Secure Data Device, Model 1900
   To remote databases: AT&T STU-III Secure Data Device, Model 1900

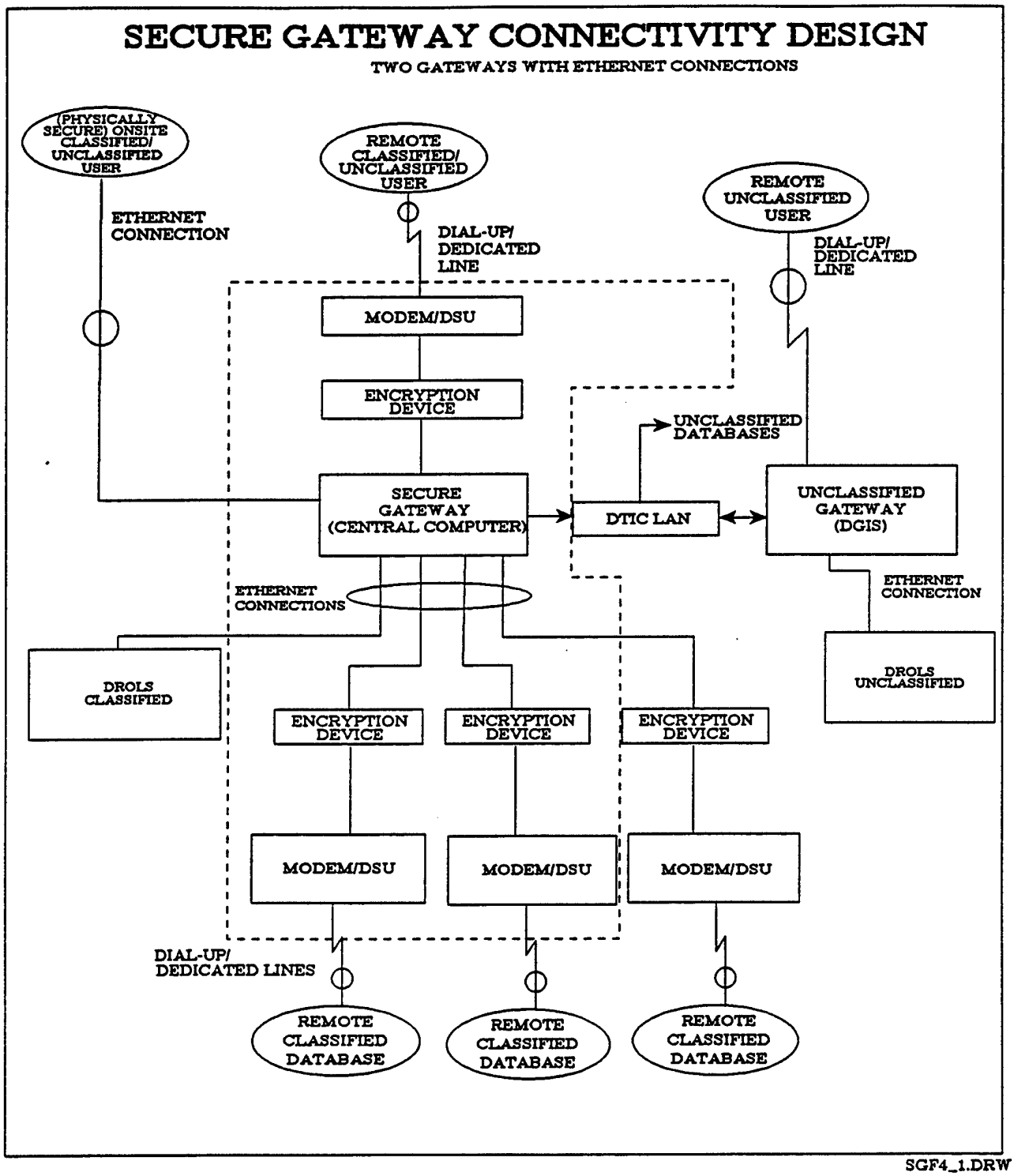


FIGURE 4.1 OPTION 1 - TWO GATEWAYS CONNECTED WITH ETHERNET
(Secure gateway is shown within dashed-line box)

4.2 OPTION 2 - TWO GATEWAYS CONNECTED WITH RS-232C

Option 2, as shown in FIGURE 4.2, is the same as Option 1 except that the connections are made with RS-232C rather than Ethernet. Ethernet connections are intended for use in networking, e.g., a secure local area network (LAN). RS-232C is intended for use in point-to-point intersystem communication connections, such as connecting a terminal or a modem to a computer. An RS-232C link allows full-duplex, serial, and asynchronous data transmission via three wires that are attached to each communicating device: transmit (output), receive (input), and common return or signal ground. "The maximum physical separation allowed between the communicating devices is 15m, and data-transmission rates are normally limited to 9600 bits/s."[7] (page 493) An advantage of using RS-232C rather than Ethernet is that the former is less expensive than the latter. RS-232C provides point-to-point connections that provide more isolation, than Ethernet would, when Ethernet is used in multi-communication path connections in a network. In contrast to Ethernet, RS-232C has the disadvantages of a relatively low bandwidth and shorter transmission distances. As for Option 1, Option 2 must be certified to at least a TCSEC B2 according to the NSA/NCSC computer security requirements publication[8]. If the user is authorized and his equipment is certified for classified communication, then the user may access the secure gateway in either a classified or an unclassified session. These communication options are shown in the FIGURE 4.2 below.

The ability to access DGIS directly will give secure gateways the ability to utilize RAM and file storage on the DGIS computer for storage of unclassified data. This will allow the secure gateway user (in unclassified mode) the capability to utilize the DGIS talking and linking facilities. These capabilities are only possible in options 1 and 2. In addition, some of the software required to access unclassified databases may be executed remotely from the DGIS computer reducing the storage, cpu and security requirements for the secure gateway.

The use of Trusted Xenix with this option satisifies most of the required functional, security, and technical characteristics (discussed in Section 2.0), including trusted E-Mail. The primary deficiencies of this configuration are that Trusted Xenix must run on an IBM AT compatible personal computer, which has an insufficient number of communication ports, and that Trusted Xenix lacks trusted "talking" and trusted "linking", without the addition of trusted application code. Also this option has the aforementioned advantages and disadvantages of RS-232C vs Ethernet.

Use of the following available technologies can be used to satisfy the required functional, security, and technical characteristics for this option of the secure gateway. This is not the only suitable set of available technologies:

1. Secure Operating System (Class B2): Trusted XENIX, or
   Secure Operating System (Class B3): XTS-200/STOP

2. Application Code:
   Application code must be custom made for the secure gateway. The extent of trusted application code required for a given secure gateway function will depend on the COTS secure operating system of the secure gateway. This trusted application code will be primarily be associated with interfacing the secure operating system with the user interface and nd communication interfaces, e.g., for the implementation of trusted "talking" and trusted "linking."

3. Facility Security: Similar to that for DTIC's DROLS

4. Platform (hardware):
   80386/80486 Personal Computer with an AT bus, or
   Dual Processor DPS 6000

5. Communications (Hardware):
   1. Connections: RS-232C

   2. Encryption Devices:
      To remote user: AT&T STU-III Secure Data Device, Model 1900
      To remote databases: DSUs/CSUs

   3. Telecommunication Devices: (Modems)
      To remote user: AT&T STU-III Secure Data Device, Model 1900
      To remote databases: DSUs/CSUs

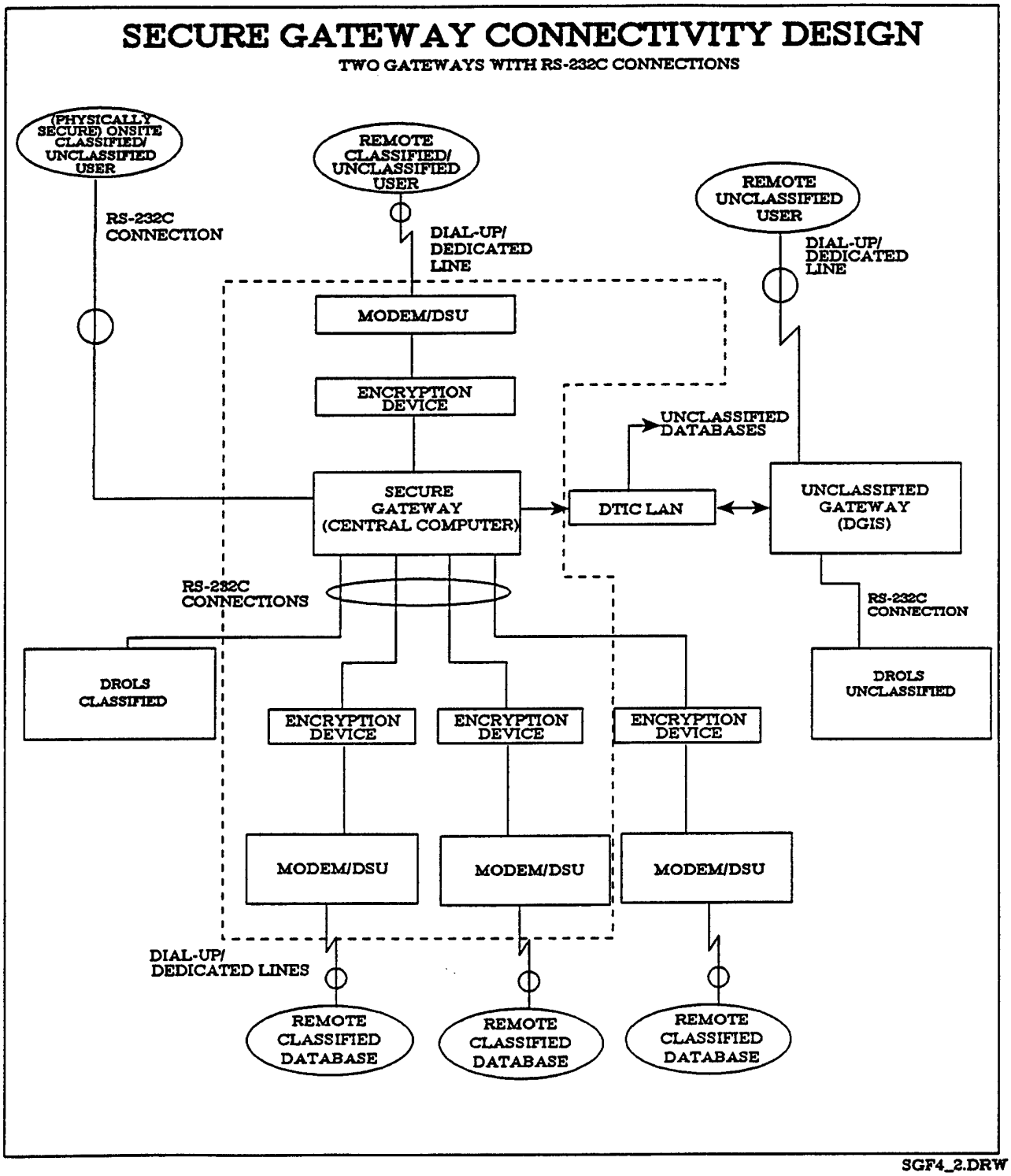


FIGURE 4.2 OPTION 2 - TWO GATEWAYS CONNECTED WITH RS-232C
(Secure gateway is shown within dashed-line box)

4.3 OPTION 3 - ONE MULTILEVEL SECURE GATEWAY

The secure gateway incorporates DGIS in the multilevel secure gateway in Option 3, as shown in FIGURE 4.3. Its connections to users and databases could use the same types of encryption and telecommunication equipment as those in Options 1 and 2. The major difference between Option 3 and the two preceding options is the incorporation of the existing DGIS within the secure gateway system. By combining the classified with the unclassified functions into a single gateway, the requirements of both current DGIS users and classified users can be satisfied with a single system. This results in requiring that Option 3 be considered to be a multilevel secure system operating in a closed security environment. A risk analysis of Option 3 results in the requirement that this configuration must be certified to at least a TCSEC Class B2 according to the NSA/NCSC computer security requirements publication[8]. As shown in the figure, if the user is authorized and his equipment is certified for classified communication, then the user may access the secure gateway in either a classified or an unclassified session.

The use of HSFI's XTS-200/STOP in this option satisifies the required functional, security, and technical characteristics (discussed in Section 2.0). The primary limitation of this configuration is the cost vs. performance of this proprietary platform from HSFI, Inc.

Use of the following available technologies can be used to satisfy the required functional, security, and technical characteristics for this option of the secure gateway. This is not the only suitable set of available technologies.

1. Secure Operating System (Class B3): XTS-200/STOP

2. Application Code:
   Application code must be custom made for the secure gateway. The extent of trusted application code required for a given secure gateway function will depend on the COTS secure operating system of the secure gateway. This trusted application code will be primarily be associated with interfacing the secure operating system with the user interface and and communication interfaces, e.g., for the implementation of trusted "talking" and trusted "linking."

3. Facility Security: Similar to that for DTIC's DROLS

4. Platform (hardware): Dual Processor DPS 6000

5. Communications (Hardware):

1. Connections: Ethernet

2. Encryption Devices: AT&T STU-III Secure Data Device, Model 1900

3. Telecommunication Devices: (Modems) AT&T STU-III Secure Data Device, Model 1900

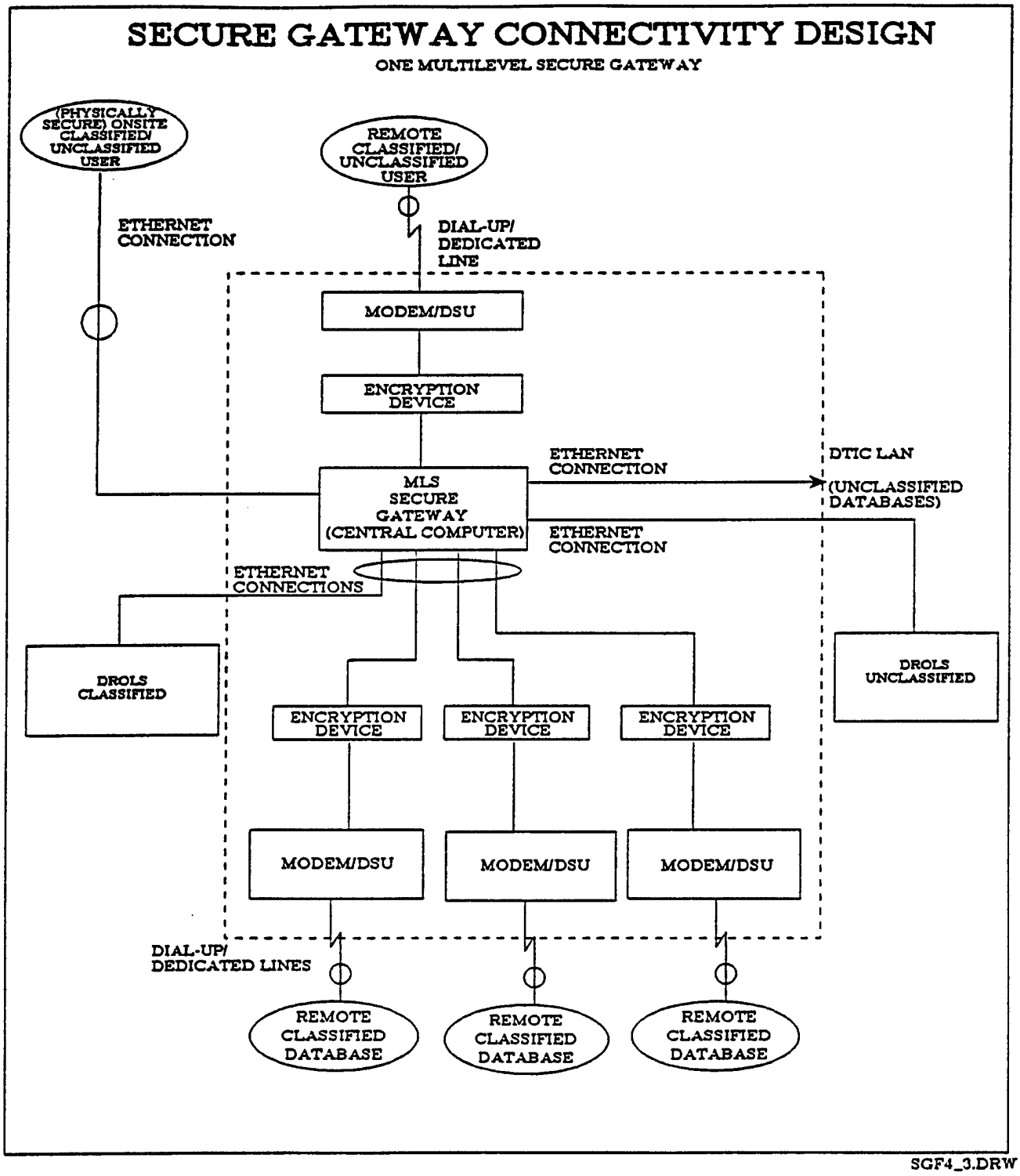


FIGURE 4.3 OPTION 3 - ONE MULTILEVEL SECURE GATEWAY
(Secure gateway is shown within dashed-line box)

4.4 OPTION 4 - MULTILEVEL SECURE (MLS) TERMINAL ACCESS CONTROLLER

A secure gateway could be configured with a multilevel secure terminal access controller, for example, one based on a Gemini computer using Gemini's Multiprocessing Secure Operating System (GEMSOS-A). The MLS terminal access controller option shown below in FIGURE 4.4 would constitute the secure gateway central computer shown in the three preceding options. This configuration consists of single classification level computers that communicate through a MLS terminal access controller, which would also function as a file server. Untrusted DGIS-like software could reside on the single level classified computers. All multilevel secure operations would be performed on the MLS terminal access controller. All accesses to the single level classified computers must be regulated by the MLS terminal access controller. This configuration would not be acceptable if multilevel classified data is present in a single level classified computer. Gemini promises to provide TCSEC Class A1 M-Component-A certification for its GEMSOS-A, which satisfy the TCSEC computer security criteria for the secure gateway. Unlike the other options, this option suffers from the restriction that the personal computers are not interchangeable, i.e., a given personal computer is restricted to operating at a single classification level.

The use of Gemini's GEMSOS-A with this option satisifies most of the required functional, security, and technical characteristics (discussed in Section 2.0). The critical limitations of this configuration are the aforementioned problems with personal computers, and that the configuration lacks trusted E-Mail, trusted "talking" and trusted "linking", without the addition of trusted application code.

Use of the following available technologies can be used to satisfy the required functional, security, and technical characteristics for this option of the secure gateway.

1. Secure Operating System (Class B3/A1): GEMSOS-A

2. Application Code:
   Application code must be custom made for the secure gateway. The extent of trusted application code required for a given secure gateway function will depend on the COTS secure operating system of the secure gateway. This trusted application code will be primarily be associated with interfacing the secure operating system with the user interface and and communication interfaces, e.g., for the implementation of trusted E-Mail, trusted "talking", and trusted "linking."

3. Facility Security: Similar to that for DTIC's DROLS

4. Platform (hardware):
   Gemini computer and
   80386/80486 Personal Computers with an AT bus

5. Communications (Hardware):
   1. Connections: Ethernet

   2. Encryption Devices: AT&T STU-III Secure Data Device, Model 1900

   3. Telecommunication Devices: (Modems)
      AT&T STU-III Secure Data Device, Model 1900

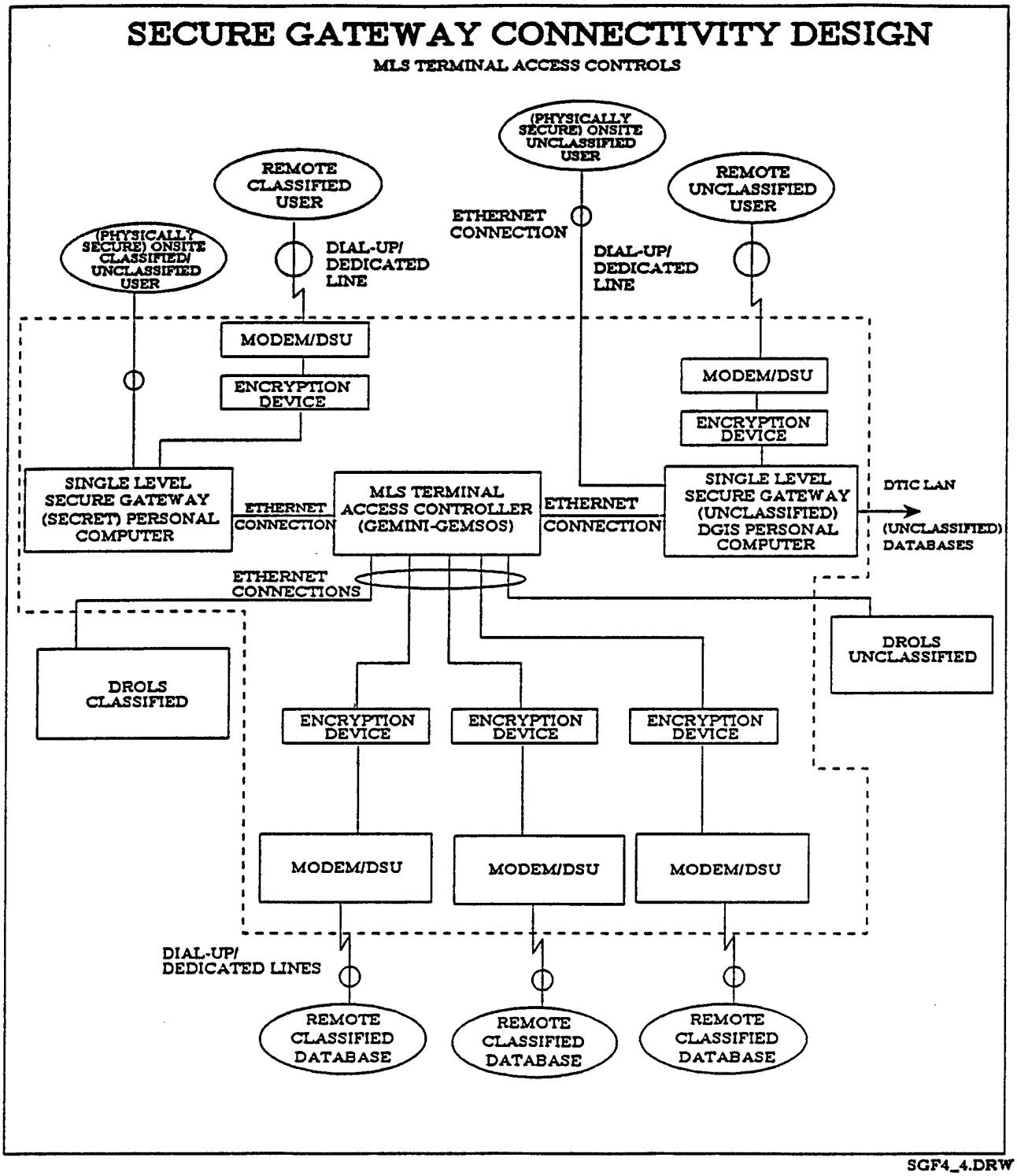


FIGURE 4.4 OPTION 4 - MLS TERMINAL ACCESS CONTROLLER
(Secure gateway is shown within dashed-line box)

4.5 OPTION 5 - MULTILEVEL SECURE (MLS) LOCAL AREA NETWORK (LAN)

A MLS LAN could be used as the central computer component of the secure gateway, which is shown for the first three options. The configuration of such a secure LAN is shown in FIGURE 4.5 below. External connections between the secure gateway and (remote) users, and between the secure gateway and (remote) databases would be through the ports of the individual computers. Inter-LAN connections would be through the secure LAN's central file server. Also this LAN file server would manage the LAN's central hard disk storage, which would hold all user files. All inter-LAN and intra-LAN connections would be via Ethernet, except for encryption devices and telecommunication connections. If the user is authorized and his equipment is certified for classified communication, then the user may access the secure gateway in either a classified or an unclassified session. These communication options are shown in the FIGURE 4.5 below. Also shown in the figure are multiple instances of personal computer nodes in the MLS LAN, which are indicated by the PC boxes behind the two PC nodes shown in the foreground. The file server's secure central hard disk storage is shown outside of the file server for clarity, but the disk storage actually resides within the file server.

The use of Trusted Xenix with this option satisifies the required functional, security, and technical characteristics (discussed in Section 2.0), including trusted E-Mail. The primary deficiency of this configuration is that Trusted Xenix lacks trusted "talking" and trusted "linking", without the addition of trusted application code.

Use of the following available technologies can be used to satisfy the required functional, security, and technical characteristics for this option of the secure gateway. This is not the only suitable set of available technologies.

1. Secure Operating System (Class B2): Trusted XENIX, or
   Secure Operating System (Class B3): XTS-200/STOP

2. Application Code:
   Application code must be custom made for the secure gateway. The extent of trusted application code required for a given secure gateway function will depend on the COTS secure operating system of the secure gateway. This trusted application code will be primarily be associated with interfacing the secure operating system with the user interface and and communication interfaces, e.g., for the implementation of trusted "talking" and trusted "linking."

3. Secure Local Area Network (Class B2): Verdix's VSLAN

4. Facility Security: Similar to that for DTIC's DROLS

5. Platform (hardware):
   80386/80486 Personal Computer with an AT bus, or
   Dual Processor DPS 6000

6. Communications (Hardware):
   1. Connections: Ethernet

   2. Encryption Devices: AT&T STU-III Secure Data Device, Model 1900

   3. Telecommunication Devices: (Modems)
      AT&T STU-III Secure Data Device, Model 1900

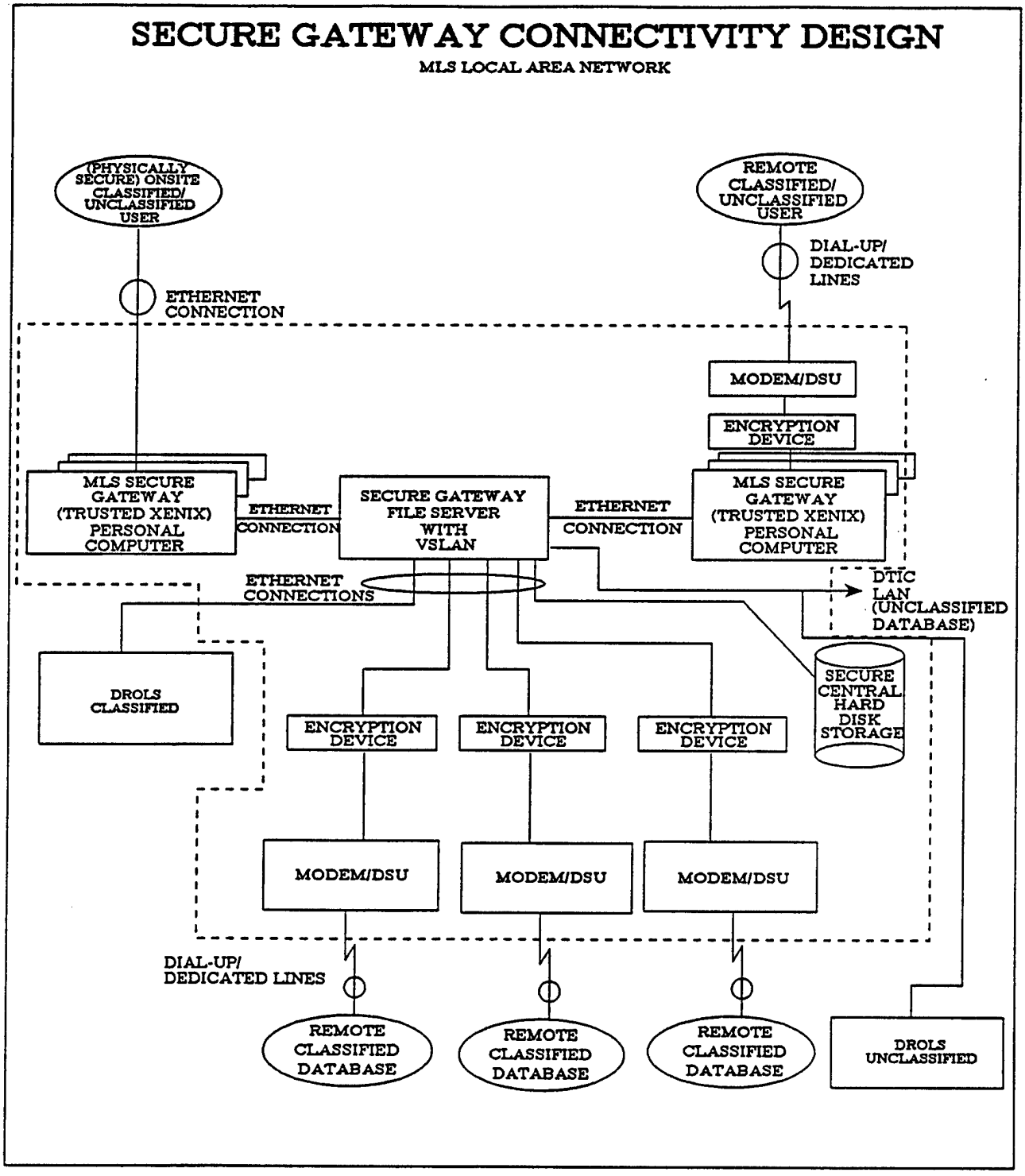


FIGURE 4.5 OPTION 5 - MLS LAN SECURE GATEWAY
(Secure gateway is shown within dashed-line box)

5.0 SYSTEM SOLUTIONS

This section presents technologies available for creating the secure gateway. Three hardware options are presented: (1) PC-based (Trusted XENIX), (2) Minicomputer based (AT&T 3B2 SYSTEM V/MLS), and (3) Superminicomputer based (HFSI's XTS-200/STOP). Refer to Appendix C for more detailed vendor information.

The availability of products that provide the technologies required for the secure gateway were identified in the second report[3] (SGT). The report concluded by proposing the following technologies for the secure gateway.

A secure gateway (conceptually) consists of: a secure operating system, a platform, communications, and application software (i.e., non-operating system software, such as the user interface). From the current effort's research into the availability of hardware and software for the secure gateway; suitable COTS products were identified for the secure operating system, the platform, and communication hardware and software. Suitable platforms can be categorized as: PC-based, or mini- or superminicomputers. Use of a mainframe system would not be cost effective for a dedicated use such as a secure gateway. Trusted E-Mail is provided by some vendors of secure operating systems. Because of the unique nature of the application software for the secure gateway, no suitable COTS application software have been found, particularly for the user interface. Therefore such application software as the user interface will have to be implemented with customized software. Existing off-the-shelf software, though not commercially available, may be adapted for implementing the user interface. In particular, the current DGIS user interface software may be suitable.

Three groups of trusted, commercially available systems or hardware are shown below. In the first three groups the systems are organized according to the size of their platforms, i.e., PC-based, and mini- or superminicomputers. After these first two groups, suitable communication devices are identified. The sets of products in the major categories are organized in the order of their technical suitability for implementing the secure gateway. Each system listed under PC-based, and Mini- or Superminicomputer is independent of the other systems in these categories. Some mix of the communication equipment shown below will be required with any PC-based, and Mini- or Superminicomputer system to complete the secure gateway, as required by future considerations. For more detailed cost information refer to Appendix C.

1. PC-based - 80386/80486 AT-compatible computer running Trusted XENIX:

   This system configuration has the hardware limitations associated with all PC-based systems, i.e., too few ports. It

has received Class B2 certification and is UNIX-like, but it lacks some capabilities required for the secure gateway, unless Trusted XENIX is run on multiple PCs. Trusted XENIX has a trusted E-Mail capability already built into it. It also has trusted "finger" and "who" commands that can serve as the basis of a trusted DGIS-like "Whoson" command. To overcome its hardware limitations, the number of available ports can be increased by adding PCs and organizing them into a secure LAN using Verdix's VSLAN. A LAN secure gateway configuration is shown in FIGURE 4.5.

80386/80486 PC with 8MB - 16MB RAM, 200 MB Drive Includes fiber transceiver and transceiver cabling	$ 5,000
Complete Trusted XENIX System	$ 3,995
Electronic Mail and Communications Extensions	
Multilevel STU-III Software	$ 390
Multilevel TCP/IP Software	$ 490

2. Minicomputer based (AT&T 3B2 SYSTEM V/MLS):

Although AT&T's System V/MLS is currently certified at the TCSEC Class B1, it does satisfy many of the Class B2 security criteria required for the secure gateway, such as sensitivity labelling. Even so, System V/MLS lacks Class B2 assurance, which may be necessary. The performance of the AT&T 3B2 may not be adequate for use in the secure gateway. The two clock speeds available are only 22MHz and 24MHz. It has been demonstrated that running the secure operating system, AT&T UNIX System V/MLS, especially with its audit trail activated, significantly degrades the performance of an AT&T 3B2 versus the performance of an AT&T 3B2 using ordinary AT&T UNIX System V. Otherwise the AT&T 3B2 System V/MLS could be used in Options 1, 2, 3, and 5 discussed in Section 4.

3. Superminicomputer based (HFSI's XTS-200/STOP VAX class):

Though all ready certified at Class B3, the performance of its current platform may not be adequate for the secure gateway.

Dual Processor DPS 6 PLUS 8 MBytes MIPS=1.7 Growth to Quad Processor 16 MBytes MIPS=3.2	$114,318

or

Dual Processor DPS 6000 PLUS 16 MBytes MIPS=5.7 Growth to Quad Processor 64 MBytes MIPS=10.0	$197,538

4. Trusted Communications Path Equipment

KG-84C General Purpose Encryption Equipment	$ 4,300
DSU/CSU	$ 900
AT&T STU-III Secure Data Device, Model 1900	$ 2,145
or	
GE STU-III/LCT 9600 Secure Communications Terminal	
single line	$ 2,540
multiline	$ 2,610

5. Secure Local Area Network

Verdix Secure Local Area Network (VSLAN):	
The Verdix Network Security Center	$ 17,500
The Verdix Network Security Device (One board per LAN Node)	$ 4,250
MLS Device Driver	$ 495
Single Level Secure (SLS) Device Driver	$ 195
Verdix Secure Internet Protocol Router (Allows connecting secure LANs)	$ 17,000

6.0 ESTIMATED SECURE GATEWAY COST

An estimate of the costs of two candidate configurations for the secure gateway is shown below. The first configuration is based on Trusted XENIX. The second configuration uses a HFSI's XTS-200/STOP VAX class superminicomputer. The costs account only for those components that are known to be required for implementing the secure gateway. Other development costs, such as for labor and technical support, are not included in the total costs shown below for these systems.

1. PC-based (Trusted XENIX) and
   Secure Local Area Network (Verdix VSLAN):

80386/80486 PC with 8MB - 16MB RAM, 200 MB Drive Includes fiber transceiver and transceiver cabling ($ 5,000 per PC, two PCs)	$ 10,000
Complete Trusted XENIX System ($ 3,995 per System, two Trusted XENIX Systems)	$ 7,990
Verdix Secure Local Area Network (VSLAN): The Verdix Network Security Center	$ 17,500
The Verdix Network Security Device ($ 4,250 per board, One board per LAN node, two LAN nodes)	$ 8,500
MLS Device Driver ($ 495 per LAN node, two LAN nodes)	$ 990
Verdix Secure Internet Protocol Router (Allows connecting secure LANs, or systems external to the secure LAN)	$ 17,000
Electronic Mail and Communications Extensions Multilevel STU-III Software ($ 390 per copy, two copies)	$ 780
Multilevel TCP/IP Software ($ 490 per copy, two copies)	$ 980
AT&T STU-III Secure Data Device, Model 1900 ($ 2145 per STU-III; 10 STU-III connections, [8 users, 2 remote database systems])	$ 21,450
TOTAL	$ 85,190

2. Superminicomputer based (HFSI's XTS-200/STOP VAX class):

Dual Processor DPS 6000 PLUS 16 MBytes MIPS=5.7 Growth to Quad Processor 64 MBytes MIPS=10.0	$197,538
KG-84C General Purpose Encryption Equipment ($ 4,300 per unit, two units for two remote database systems)	$ 8,600
DSU/CSU ($ 900 per unit, two units for two remote database systems)	$ 1,800
AT&T STU-III Secure Data Device, Model 1900 ($ 2145 per STU-III; 8 STU-III connections for 8 users)	$ 17,160
TOTAL	$225,098

7.0 CERTIFICATION

The certification process must be defined by the secure gateway's designating approving authority (DLA and/or NSA/NCSC). The TCSEC[1] states the following about the evaluation process in its Appendix A, "Commercial Product Evaluation Process" (page 89):

"The evaluation provides a key input to a computer system security approval/accreditation. However, it does not constitute a complete computer system security evaluation. A complete study (e.g., as in reference[9] [Guideline for Computer Security Certification and Accreditation]) must consider additional factors dealing with the system in its unique environment, such as its proposed security mode of operation, specific users, applications, data sensitivity, physical and personnel security, administrative and procedural security, TEMPEST, and communications security."

The following is a list of basic steps in the certification process for the secure gateway.

1. Analysis and design must be coordinated with DLA. DLA may also require coordination with NSA/NCSC.

2. Building the secure gateway must be guided by the certification requirements.

3. Test the secure gateway for certification according to the specified DLA and/or NSA/NCSC test plan.

4. Secure operation of the secure gateway will be the responsibility of its system security administrator.

5. The secure gateway and its system security administrator will not be responsible for the security and integrity of information once it has arrived at a remote user's site. The security and integrity of such information becomes the responsibility of the remote user and the security officers at the user's site.

6. Recertification of the secure gateway will be required only if modifications or enhancements are made to the secure gateway's trusted software. Modifications or enhancements to (application) software outside of the secure gateway's TCB will not warrant recertification of the secure gateway.

---

[9] Federal Information Processing Standards Publication (FIPS PUB) 102, Guideline for Computer Security Certification and Accreditation.

8.0 CONCLUSION

This report presents the results of a study of the feasibility of developing a secure gateway. Three types of characteristics required for the secure gateway were discussed, i.e., functional, security, and technical characteristics. To provide assurance of the technical feasibility of a secure gateway, TCB components were mapped to secure gateway features. Then various configuration options for developing a secure gateway were presented. System solutions for developing a secure gateway were then offered, which were followed by estimated component costs for a secure gateway. The cost of three configurations for implementing the secure gateway were offered as system solutions. Last, the certification process for a secure gateway was presented. The certification process of the gateway must be determined by the gateway's designated approving authority (DLA and/or NSA/NCSC).

In the short term, at least, the secure gateway configuration, Option 5 is the most viable. Option 5 is the most cost effective option to achieve the desired performance while satisfying the security and functional requirements of the secure gateway. Because Option 5 is based on a MLS LAN, it can be more easily expanded than the other options. As stated earlier, Option 4, the MLS terminal access controller, suffers from the restriction that the personal computers, as used in this option, are not interchangeable, i.e., a given personal computer is restricted to operating at a single classification level. Option 4, even if it were technically acceptable (which is questionable), is not as cost effective as Option 5. Option 3 is more desirable than either Options 1 and 2, because it integrates classified and unclassified database accesses on a single central computer. The critical problem with Option 3, that makes it unacceptable, at this time, is that it would require trusted operating system on a (super)mini class of computer. Smaller personnal conputers lack the communications capabilities and throughput to satisfy numerous simultaneous users. HFSI's XTS-200/STOP on any DPS platform, is such a system, but this system currently lacks the required performance for the secure gateway and it is not as cost effective as Option 5. The performance of this system will soon be surpassed when Trusted Mach is available on (super)mini class computers, based on industry standard processors that will exceed the performance of HFSI's proprietary processor. Option 1 is better than Option 2, because Ethernet allows for connections to be made over longer distances, using a higher bandwidth, and with higher transmission rates. Even if a short term solution is chosen, using a secure LAN (Option 5), Trusted Mach can be phased into this platform later.

This study concludes that a Class B2 secure gateway can be developed with existing technology. Of the options reviewed, a secure gateway based on a multilevel secure local area network could provide the required performance at the best cost of

"commercial-off-the-shelf" products. The essential technologies for this option are Trusted XENIX, Verdix's VSLAN, and Ethernet connections. Trusted XENIX is a certified Class B2 trusted (UNIX) operating system, that can be used on personal computers based on the Intel 80386 or 80486 processors. VSLAN is a certified Class B2 secure local area network that can be used with Trusted XENIX to provide a secure gateway with the required performance.

If the secure gateway's development were delayed until Trusted Mach is available, this secure operating system could serve to provide a more affordable standardized trusted environment than can be achieved with currently available certified operating systems. Also, Trusted Mach is anticipated to be certified higher than Class B2.

Crucial to implementing the secure gateway is the demonstration of application software that has the required "hooks" to the underlying secure operating system. The rest of the gateway consists of hardware and software technology that already exists or will become available in the foreseeable future. The incorporation of the remote access communication channels in the secure gateway should also be straightforward.

The following list is a summary of basic issues regarding the technology of developing a secure gateway. With these issues are their resolutions by the use of the indicated TCB mechanism(s).

Summary of Basic Issues and their Resolution

- Users must not be allowed to have direct access to databases, so as to bypass the secure gateway's TCB.

  Satisfying TCB mechanism: Secure Operating System

- Memory and disk storage must be partitioned according to user authorization and classification

  Satisfying TCB mechanism: Secure Operating System

- E-Mail, "Talking", and "Linking"

  Satisfying TCB mechanism: Secure Operating System, Trusted Application Code, and Trusted Communication Paths

- Multilevel secure citation management

  Satisfying TCB mechanism: Secure Operating System

- Communication Interfaces

  Satisfying TCB mechanism: Secure Operating System, Trusted Application Code, and Trusted Communication Paths

References

1 U.S. Department of Defense (DoD), Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200.28-STD, December 1985.

2 Buchanan, George, and Steven Goldstein, Security Regulations Relevant to Developing and Using a Secure Gateway, IIT Research Institute, February 1992.

3 Buchanan, George, and Steven Goldstein, Evaluation of Current Technologies for Developing a Secure Gateway, IIT Research Institute, February 1992.

4 Defense Technical Information Center (DTIC), Gateway User Support and Training Office, DGIS Users' Guide, (DoD Gateway Information System), August 1989.

5 National Computer Security Center, Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria (TNI) (NCSC-TG-005 Version-1), 21 July 1987.

6 National Security Agency, System Security Policy for the Security Enhanced DoD Gateway Information System, October 28, 1991.

7 Hayes, John P., Computer Architecture and Organization, 2nd Edition. New York: McGraw-Hill, 1988.

8 DoD Computer Security Center (DoDCSC), Computer Security Requirements - - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments (CSC-STD-003-85), 25 June 1985.

9 Federal Information Processing Standards Publication (FIPS PUB) 102, Guideline for Computer Security Certification and Accreditation.

APPENDIX A

LIST OF ACRONYMS

ACL - Access Control List

ACMW - Addamax 386 Compartmented Mode Workstation

CASS - Commodity Application Services System (XTS-200/STOP)

COMSEC - computer security

COTS - "commercial-off-the-shelf"

CIK - Crypto Ignition Key (GE STU-III/LCT 9600)

CSTI - Communications Systems Technology, Inc.

CSU - Channel Service Unit

DAC - Discretionary Access Control

DDN - Defense Data Network

DES - Data Encryption Standard (Verdix's VSLAN)

DGIS - DoD Gateway Information System

DIA - Defense Intelligence Agency

DLA - Defense Logistics Agency

DoD - Department of Defense

DROLS - Defense RDT&E Online System

DSU - Data Service Unit

DTIC - Defense Technical Information Center

ECPL - Endorsed Cryptographic Products List

EPL - Evaluated Products List

FTP - File Transfer Protocol

GEMSOS - Gemini [Multiprocessing] Secure Operating System

IP - Internet Protocol

LAN - Local Area Network

LCT - Low Cost Terminal ([AT&T] STU-III LCT)

MAC - Mandatory Access Control

MLS - multilevel secure

MTBF - mean time between failure

NCSC - National Computer Security Center

NSA - National Security Agency

NSC - Network Security Center

NSD - Network Security Device (Verdix's VSLAN)

OSI - Open Systems Interconnection (Verdix's VSLAN)

RAMP - (NSA/NCSC) RAting Maintenance Phase (System V/MLS)

SACS - Secure Access Control System (AT&T STU-III, Model 1900)

SCCS - Source Code Control System ([Addamax] Trusted i386 UNIX Compartmented Mode Workstation)

SGSR - Security Regulations Relevant to Developing and Using a Secure Gateway

SGT - Evaluation of Technologies for Developing a Secure Gateway

SMTP - Simple Mail Transfer Protocol

SNS - Secure Network Server (Boeing MLS LAN)

STU - Secure Telephone Unit

SVID - System V Interface Definition (System V/MLS)

SVVS - System V Verification Suite (System V/MLS)

TCB - Trusted Computing Base

TCP - Transmission Control Protocol

TCSEC - (DoD) Trusted Computer System Evaluation Criteria

TED - Truck Encryption Device (KG-81)

TNI - Trusted Network Interpretation (of the TCSEC)

UDP - User Datagram Protocol (Boeing MLS LAN)

WAN - Wide Area Network

APPENDIX B

SYSTEM SECURITY POLICY

System Security Policy
for the
Security Enhanced DoD Gateway Information System
December 20, 1991

1.0 Introduction

1.1 Definition

System Security Policy is defined as "The set of security objectives that regulate a given system's management, protection and distribution of sensitive resources."

1.2 Purpose

The purpose of this system security policy document is to provide a specific set of system security objectives which are to be observed by the Security Enhanced DoD Gateway Information System (SEDGIS) in its determination of applicable security operational concepts, requirements, design, development, implementation, testing, and quality assurance. These objectives are intended to ensure that while processing, storing, using, or distributing sensitive resources, the SEDGIS will, with reasonable dependability, comply with all applicable Government laws, rules, and practices as stated in this policy document.

1.3 Scope

This policy document contains all system security objectives related to the SEDGIS. This policy document is intended to be design independent and is not limited to any particular system design. However, it does address the intended operational mode of the SEDGIS which is multi-level secure.

2.0 References

(a) DoD 5200.1-R, "DoD Information Security Program Regulation," June 1986

(b) E.O. 12356, "National Security Information," April 2, 1982

(c) DoD 5200.2-R, "DoD Personnel Security Program," December 1979

(d) DRAFT "National Security Telecommunications and Information System Security Glossary," August 2, 1991 - Currently under review by the NSTISSC.

(e) DoDD 5100.55, United States Security Authority for North Atlantic Treaty Organization Affairs, April 21, 1982.

(f) United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN) Instruction 1-69, United States Implementation of NATO Security Procedures, Enclosure 2 to DoD Directive 5100.55.

(g) Office of Secretary of Defense Memorandum dated 26 July 1988, Subject: Handling of NATO RESTRICTED Information.

3.0 System Description

The Security Enhanced DoD Gateway Information System, SEDGIS, is a research tool designed to help scientists, engineers, and information specialists of the United States Government and it's contractors take greater advantage of the wealth of information resources that are currently available.

The primary purpose of SEDGIS is to help remote users access diverse bibliographic databases at geographically disperse locations and retrieve, analyze, sort, and reformat bibliographic citations. The SEDGIS supports the searching and retrieval of bibliographic citations based upon search statements submitted by the user which identify the databases to be searched and the search parameters (i.e. author, subject, title, abstract words, etc.) to be used. The SEDGIS permits the user to request post-processing to analyze, sort, or reformat bibliographic citations. Users may also submit requests for documents to libraries and information organizations through SEDGIS. The delivery of documents to users is handled independently of SEDGIS by the libraries and information organizations maintaining the documents.

Bibliographic databases contain references to written material such as books, journal articles, technical reports, conference proceedings, patents, and studies. A bibliographic citation identifies where to find referenced work. Each bibliographic citation consists of author name(s), title, publication year, source of the publication (journal reference, publisher name, patent assignee), index terms, and an abstract.

The information processed by the SEDGIS may be unclassified or classified as NATO Restricted, Confidential, or Secret. SEDGIS also processes propriatary information which must be protected. Classifications are associated with each field of a bibliographic citation and with index terms.

Secondary capabilities provided by the SEDGIS are editing and mail services. Editing capabilities are provided by the SEDGIS to permit users to edit information produced as a result of their requests for bibliographic searches and analyses and to generate messages for delivery to others. The mail facility permits users to send and receive messages among themselves and with others who are located on systems that maintain communications with SEDGIS but who are not authorized to use the

SEDCIS services and resources. The editing and mail services are not to be used to process information which is out of the classification range stated above.

4.0 Security Policy

4.1 Definitions

The terms used within this document are defined within DoD 5200.1-R unless otherwise stated within this section.

Data Integrity - Condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. Reference d.

NATO RESTRICTED - a classification as defined within reference f and by E.O. 12356.

System Integrity - Quality of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. Reference d.

4.2 Security Classification Designations

Designations for the classification of U.S. controlled information or material that requires protection against unauthorized disclosure in the interest of national security are defined within DoD 5200.1-R.

Designations for the classification of NATO RESTRICTED information are contained within DoDD 5100.55.

4.3 Safeguarding

The system shall afford classified information the level of protection against unauthorized disclosure commensurate with the level of the classification assigned. This protection shall be afforded under the varying conditions that may arise in connection with the use, dissemination, storage, movement or transmission, and destruction of classified information within the system.

The U.S. does not have a security classification equivalent to "NATO RESTRICTED." NATO RESTRICTED information shall be safeguarded in a manner that shall prevent disclosure to nongovernmental personnel.

Information that is marked as Contractor Proprietary shall be safeguarded in a manner that shall prevent disclosure to nongovernmental personnel.

4.4 Authority to Classify

The system shall be responsible for the derivative application of classification markings to all information generated by the system in which the system has incorporated or generated in new form, information that is already classified by an original classification authority. The system shall:

a. Respect the original classification decisions;

b. Verify the information's current level of classification as far as practicable before applying the markings; and

c. Carry forward to any newly created information any additional markings.

The system shall have no declassification, downgrading, or regrading capabilities.

4.5 Classification Principles, Criteria, and Considerations

Information extracted from a classified source shall be derivatively classified or not classified by the system in accordance with the classification markings shown in the source. The overall and internal markings of the source should supply adequate classification guidance. If internal markings or classification guidance are not found in the source, and no reference is made to an applicable and available classification guide, the extracted information shall be classified according either to the overall marking of the source, or guidance obtained from the classifier of the source material.

4.6 Marking

Information determined to require classification protection under DoD 5200.1-R shall be so designated within the system. Designation by means other than physical marking may be used, but shall be followed by physical marking as soon as possible.

Designation by physical marking, notation, or other means serves to warn the holder about the classification of the information involved; to indicate the degree of protection against unauthorized disclosure that is required for that particular level of classification.

4.7 Specific Marking of Information

The overall classification of each information unit generated by the system shall be appropriately marked and the markings bound to the information. Each component of an information unit shall be appropriately marked according to the content, to include "Unclassified" when no classified information is contained in the component. When elements of information in

one portion require different classifications, but segregation into separate portions would destroy continuity or context, the highest classification required for any item shall be applied to that portion.

NATO RESTRICTED information contained within U.S. classified information shall be identified by applying the appropriate U.S. and NATO markings to the component. The overall information unit shall bear the U.S. classification with the further marking that the unit contains NATO RESTRICTED information.

When NATO RESTRICTED information is included in U.S. unclassified information units generated by the system, the unit shall be marked to indicate that NATO RESTRICTED information is contained within the unit.

4.8 Safekeeping and Storage

The system shall store classified information only under conditions adequate to prevent unauthorized persons from gaining access to the information.

4.9 Access

The system shall prevent users from acquiring access to classified information unless the users have the appropriate security clearance and need-to-know for the information. The final responsibility for determining whether a user's official duties require possession of or access to any element or item of classified information, and whether the user has been granted the appropriate security clearance by proper authority, rests with the system.

Contractor Proprietary and NATO RESTRICTED information will be available only to U.S. government personnel with a need-to-know for the information.

4.10 Dissemination

Standing distribution requirements for Secret and Confidential information and materials, such as distribution lists, shall be reviewed by the system at least annually to verify the recipients' need-to-know.

4.11 Accountability and Control

The system shall have established the appropriate procedures and mechanisms for controlling SECRET information received, generated, distributed, or destroyed by the system. The controls placed on SECRET information by the system must meet the following minimum requirements:

a. It must provide a means of ensuring that SECRET information sent outside the system has been delivered only to the intended recipient.

b. It must provide a record of receipt and dispatch of SECRET material by users.

c. Records of the receipt and dispatch of SECRET material shall be retained for a minimum of 2 years.

Procedures and mechanisms shall be established to protect CONFIDENTIAL information received, generated, distributed, or stored by the system.

4.12 Information Integrity

The system shall maintain the consistency and accuracy of information accepted into the system's control and protect that information from unauthorized modification or destruction.

4.13 System Integrity

The system shall ensure that the services and resources provided by the system are logically correct and reliable.

5.0 Assumptions

Assumption 1: Information available to the system has been classified by an original classification authority according to the applicable policies and guidelines and is appropriately marked. The system does not originate information for user consumption as part of the service and is not an original classification authority.

Assumption 2: The information the system accesses to generate responses to user queries is not maintained by the SEDGIS. Citations placed in those information bases are understood to be maintained and appropriately classified by mechanisms outside the SEDGIS.

Assumption 3: The system shall process both unclassified and classified information. Information classifications shall include NATO Restricted, Confidential, and Secret. Contractor proprietary data shall also be processed by the system. No compartmented information will be processed by the system.

Assumption 4: Aggregation of data and data inference are acknowledged as security concerns, but there exist no current policies or mechanisms to address these concerns. Until policies and mechanisms addressing these issues are developed, the DGIS will not address the issues.

Assumption 5: User security clearances are determined and assigned by the appropriate organization as outlined in DoD 5200.2-R and are not assigned by the DGIS. The DoD organization sponsoring a user identifies the user's clearance and provides the supporting documentation to the DGIS through the appropriate channels.

Assumption 6: Need-to-know is determined by the U.S. government organization sponsoring a user of the DGIS and provided to DGIS in terms of fields and groups of interest. DGIS enforces need-to-know on fields and groups of interest for classified information only.

Assumption 7: Users who receive classified information from the DGIS will appropriately protect that information. The system is not responsible for protecting information that has been released to the user. The system will protect all copies of information and records of receipt of classified information to the appropriate level until that information is appropriately destroyed within the system.

Assumption 8: There are no stringent availability requirements for the DGIS, as it is not consider to be a critical system. They do have requirements that the system provide reasonable service to all users, but it is not consider a critical security problem if it does not.

Assumption 9: The Accreditor for the DGIS is the Defense Logistics Agency and those accrediting authorities of systems with which the DGIS interacts.

SYSTEM SECURITY SPECIFICATION
DRAFT OUTLINE
for the
SECURITY ENHANCED DOD GATEWAY INFORMATION SYSTEM
19 December 1991

1 Introduction

1.1 Purpose

This system security specification should provide a mid-level overview of the Security Enhanced Department of Defense Gateway Information System (SEDGIS) security requirements. This document should map closely with the System Security Policy for SEDGIS and will serve as the foundation for the development of the system security architecture.

1.2 Scope

The system security specification shall stay within the following limits:

- It must present the technical security requirements of the system as a whole.
- It must not be the requirements of the individual components.
- It may be based upon knowledge that the system is made up of individual pieces, but may not be based upon the knowledge of which pieces make up the system.
- It must be consistent with the system security policy.
- It must be a problem statement, not a solution statement.

2 References

(a) Executive Order 12356, "National Security Information," April 2, 1982

(b) NTISSI 7000, "TEMPEST Countermeasures for Facilities," 17 October 1988

(c) DoD 5200.1-R, "DoD Information Security Program Regulation," June 1986

(d) DoD 5200.2-R, "DoD Personnel Security Program," December 1979

(e) DoD 5200.28, "Security Requirements for Automated Information Systems," 21 March 1988

(f) DoD 5200.28-STD, "DoD Trusted Computer System Evaluation Criteria," December 1985

(g) CSC-STD-003-85, "Computer Security Requirements, Guidance for Applying the DoD Trusted Computer System Evaluation Criteria in Specific Environments," 25 June 1985

(h) DoD 5200.5, "Communications Security," 21 April 1990

(i) DoD 5200.19, "Control of Compromising Emanations," 23 February 1990

(j) "System Security Policy for the Security Enhanced DoD Gateway Information System," 2 December 1991

3 Definitions

Accreditation Range: A set of compartments and classifications that a component is accredited to process and keep separated.

Citation: The bibliographical reference SEDGIS sends to users in response to a query which includes fields for an index number, title, author, topic, abstract, and publication date.

Citation Field: Individual field (such as the "topic" field used to determine need-to-know) within a citation.

Classified Information: Any information which is marked Confidential, Secret, or Top Secret in accordance with E.O.12356.

Computing Session: Any and all system activities performed by a user from the time the user logs in to a system until the user logs off the system.

Data Origin Authentication: The corroboration that the source of data received is as claimed.

Information Unit: Any collection of data which is treated as an individual entity for access control purposes.

Peer Entity Authentication: The corroboration that a peer entity in an association is the one claimed.

Restricted Information: Data which only authorized persons may use. In SEDGIS, this refers to information marked Proprietary, NATO RESTRICTED, and nuclear.

Security Critical Elements: Elements of a system, whose correct operation is required to prevent events from occurring that may be contrary to the security policy of the system. For example, error detection and correction circuitry for primary memory would be considered a security critical element. Failure of this element could result in an undetected memory error changing a vital table entry that would allow access by a process to unauthorized data.

Sensitivity Marking: Those markings necessary to denote the protection to be afforded information. For this system, those markings are SECRET, CONFIDENTIAL, NATO RESTRICTED, UNCLASSIFIED, and/or PROPRIETARY.

System Protection Mechanisms: Elements within a system that are used to enforce the policy decisions made by the system.

Topic Field: One field of a citation which contains terms or key words to be used for need-to-know determinations.

Unclassified Information: Information which is not classified or restricted information.

4 System Description

The following is a system-level description of the various user and source links connected to the SEDGIS gateway (FIGURE 4.0).

SEDGIS will accommodate a large number of users who can be geographically dispersed. Users of the SEDGIS service will operate in either the MLS or system-high mode. The user's clearances may range from Unclassified to Top Secret. Users create and send queries. When the queries are returned, the user may then perform some post-receipt processing of the results. Users are also provided an E-mail service which allows communication with users on SEDGIS and other systems. SEDGIS users will be differentiated as either U.S. government personnel or contractors. Government personnel may be allowed access to query responses that contain proprietary and/or NATO RESTRICTED information, while contractors are not.

There are three database sources connected to the SEDGIS Gateway. They are Dialog, DROLS-Classified, and DROLS-Unclassified. Of these, Dialog and DROLS-Unclassified are unclassified and DROLS-Classified ranges from Restricted to Secret. DROLS-Classified and DROLS-Unclassified belong to the Defense Logistics Agency. Dialog is a commercial database.

SEDGIS is capable of providing E-mail and TELNET connections to unclassified networks such as "Internet" and classified networks such as "DS-Net 1". Users may also query through the Internet and DS-Net 1.

4.1 System Boundaries

The SEDGIS system boundaries will include the Gateway and those communications links plus their hardware/software interfaces which provide a level of protection afforded classified and/or restricted information. These links will include those links that connect MLS and system high users to SEDGIS, the links from the DROLS-Classified database since classified and/or restricted information can be relayed, and the links needed for classified E-mail. Links to strictly unclassified (no classified or restricted) users, networks, and databases are afforded no protection beyond that provided by the existing carrier and, therefore, are not considered under the purview of this system. SEDGIS can accept queries over a link below the clearance level of the user. SEDGIS can then process the query and assemble results containing data at or below the clearance of the user. SEDGIS will only send these results over links protected at or above the classification level required for the sensitivity of the information.

Only pre-determined, authorized software will be used within the security system portion of SEDGIS to execute the functions of the system which are query, post-processing, and E-mail. The system will not execute user programs.

4.2 INFOSEC Risk Analysis and Abatement

4.2.1 INFOSEC Solutions

Cryptographic types and levels of trust are used only to provide a shorthand way of establishing minimum levels of protection. Other protection mechanisms which provide similar or greater levels of protection, including techniques besides COMSEC and COMPUSEC (e.g., protected wire distribution system) should be considered acceptable.

The SEDGIS security needs identified below are typical of classified systems with a mix of data communication and data processing elements. When analyzing the SEDGIS system, a combination of requirements is exhibited which collectively can be identified as cryptographic types and computer security levels of trust. It is not necessarily true that every component must be a Type I cryptographic component or a B3 computer component in order for the system to meet its minimum Type I and B3 requirements. Nonetheless, each component of the system must be selected according to its ability to contribute appropriately to the system security requirements.

4.2.2 Communications

Because various users of the SEDGIS are cleared to download classified information through the system (from the DROLS database), and since secure communications will be involved, at least Type I cryptography will be required. Type 2 cryptography may also be required to protect unclassified U.S. government users since they will be authorized to receive proprietary and/or NATO RESTRICTED information. Cryptography requirements for the SEDGIS operating environment will be further analyzed in section 5.1 on cryptographics. Key management requirements are discussed in section 5.2.

4.2.3 Computing

The DTIC MLS library service is intended to operate in no less than a security domains (B3) level of trust as defined in DoD 5200.28-STD based on the following criteria:

Rmax (3) Secret with no categories
- Rmin (0) Uncleared
risk index=3 (B3)

The prescribed minimum level of trust for this case is B3 since the SEDGIS system operates in an OPEN environment. Secure computing requirements are discussed in section 6.

4.2.4 TEMPEST

SEDGIS shall comply with the TEMPEST standards as described in NTISSI 7000.

5 Communication Security

Classified or restricted information that is in transit between SEDGIS and its users, that is not protected by physical means, will be protected using an NSA approved cryptographic device.

5.1 Cryptographics

Regarding cryptographics, SEDGIS shall adhere to the following constraints:

- The highest level of classification of information in the SEDGIS is Secret.

- The cryptographic devices must provide protection of information in transit against disclosure to unauthorized personnel.

5.2 Key Management

When using NSA approved cryptographic devices for protection of classified or restricted information, NSA-provided Cryptographic Keying material shall be used. A Cryptographic Key Management Account must be identified for proper management of this Keying Material.

5.3 Equipment Safeguards

Cryptographic devices/materials require protection against access, tampering, and modification, by unauthorized personnel. This protection will be afforded while unattended, in storage, and in transit in accordance with governing laws, policies, and instructions.

5.3.1 Compromise Recovery

System documentation shall specify what measures will be taken to recover system security when devices/material are compromised (e.g., lost, stolen, modified, tampered, etc.).

6 Computer Security

6.1 Classification Principles, Criteria, and Considerations

SEDGIS shall ensure the following:

1. any existing sensitivity markings received from service providers are maintained;

2. appropriate markings are carried forward to newly created information; and

3. any data transferred within the library system maintains its existing sensitivity marking.

If material is included which has no sensitivity marking or is obviously mis-marked it shall be handled as if it were SECRET and either purged from the system or held for review by system administration personnel.

If material is included which has no internal sensitivity markings, the extracted information shall be marked at either the overall classification of the material, or in accordance with guidance from the original classifier of the material.

The system shall have no original classification authority.

All E-mail messages must have appropriate sensitivity

markings.

6.2 Specific Marking of Information

Any classified or restricted information must be appropriately designated within the system. Designation by means other than physical markings may be used, but shall be followed by physical markings whenever a hardcopy is produced. All removable media containing classified or restricted information shall be physically marked.

The system shall be capable of identifying, for security reasons, the beginning and end of each computing session, E-mail message, citation, and citation field. Information of an unclassified nature shall be appropriately marked. When citation fields contain information of varying classification levels, the entire citation shall be marked at the highest classification level of information in the citation fields.

If material which lacks a sensitivity marking is to be imported, SEDGIS must query the user and receive a reply designating the sensitivity marking to be applied. The sensitivity marking must be one which the system recognizes i.e. SECRET, CONFIDENTIAL, NATO RESTRICTED, UNCLASSIFIED, and/or PROPRIETARY. If the sensitivity marking is not one which the system recognizes, the material shall not be imported by the system. The sensitivity marking must be consistent with the user's authorized accesses.

Sensitivity markings associated with each system resource shall be maintained by SEDGIS. These markings shall be used as the basis for all access control decisions. The clearance level of the user shall be compared to the sensitivity marking of data requested and a determination made whether the user is authorized access to the data.

6.2.1 Integrity of Sensitivity Markings

Sensitivity markings shall accurately reflect the sensitivity marking of information with which they are associated. When exported by SEDGIS, the sensitivity markings shall accurately and unambiguously represent the sensitivity marking of information with which they are associated.

6.2.2 Marking Hardcopy Output

The SEDGIS system administrator shall specify the printable marking names associated with the classification levels used by the system. SEDGIS shall properly mark the beginning and end of all hardcopy output with the appropriate term to accurately reflect the overall sensitivity of the unit of output. SEDGIS shall mark the

beginning and end of each page of hardcopy output with the appropriate term to accurately reflect the overall sensitivity of the data/information on the page. Any override of these page marking defaults shall be auditable by SEDGIS.

6.3 Exportation of Information

SEDGIS will designate each communication channel and I/O device as either single-level or multilevel. Any change to the status of these outputs will be done manually and will be auditable. Additionally, changes to the security levels will be auditable.

6.3.1 Exportation to Multilevel Devices

When the SEDGIS is sending information to an I/O device the sensitivity marking of that information shall also be sent. It will reside on the same physical medium and in the same form (i.e., machine-readable or human-readable). When the SEDGIS is sending or receiving information over a multilevel communication channel, the protocol used on that channel shall clearly match the sensitivity marking with the associated information that is being sent or received.

6.3.2 Exportation to Single-Level Devices

Single-level I/O devices and single-level communication channels are not required to maintain sensitivity markings. However, the SEDGIS shall include a mechanism by which the SEDGIS and an authorized user reliably communicate to designate the single sensitivity marking for the information being sent or received.

6.3.3 Importation from Multilevel Devices

When SEDGIS receives information from a storage or I/O device, the sensitivity marking of that information shall also be received. It will reside on the same physical medium and in the same form (i.e., machine-readable or human-readable). When the SEDGIS is sending or receiving information over a multilevel communication channel, the protocol used on that channel shall clearly match the sensitivity marking with the associated information that is being sent or received.

6.3.4 Importation from Single-Level Devices

Single-level I/O devices and single-level communication

channels are not required to maintain sensitivity markings. However, the SEDGIS shall include a mechanism by which the SEDGIS and an authorized user reliably communicate to designate the single sensitivity marking for the information being sent or received.

6.4 Accreditation Range

Each component shall have a designated accreditation range. The system shall ensure that all information sent to a component is within the accreditation range for that component.

6.5 Access

The SEDGIS shall prevent users from acquiring access to classified or restricted information unless the users have the appropriate security clearance and need-to-know for the information. To enforce the access decisions, the system shall be provided with each user's security clearance and a listing of the topics of information the user requires from a U.S. Government sponsor authorized to register users. All information processed by the SEDGIS will have an associated classification. SEDGIS shall enforce access decisions based upon the topic and classification of information requested and the information registered about the user requesting access.

6.6 Classification/Clearance

Information in SEDGIS shall display one of the following sensitivity markings: UNCLASSIFIED, NATO RESTRICTED, CONFIDENTIAL, or SECRET. Each user must possess a valid security clearance for the most restricted level of information which that user can access. Users will be treated as either uncleared or cleared to the NATO RESTRICTED, CONFIDENTIAL or SECRET level. Users shall also be able to read information of a lower classification than the level of clearance held.

6.6.1 Proprietary Information

Users will either be employees of the U.S Government or its contractors. Information may also be designated as PROPRIETARY with access limited to U.S. Government employees with a Confidential or Secret clearance.

6.6.2 Need-to-know

A static set of topic fields has been established to identify information. All information in the system shall be assigned to one or more of these topic fields. Each user shall be able to

access only that information for which the user has a valid need-to-know. A user's need-to-know shall be determined by the user's government sponsor. The user's need-to-know shall be registered for each set of topic fields. Need-to-know privileges shall be periodically reviewed and updated.

Need-to-know for electronic mail messages is determined by the originator of the message. Electronic mail messages shall be accessible only to the originator and the addresses of the message.

Files shall be accessible only to the file owner and those users who the owner designates as having a need for the information.

6.7 Accountability and Control

SEDGIS shall provide accountability by maintaining and protecting information tracing all actions affecting security to the responsible party. This shall be done by ensuring that all users connected to SEDGIS are identified and that an audit log is kept and secured.

6.7.1 Identification and Authentication

SEDGIS shall identify and authenticate all users before allowing users to access information in the system or before performing any other actions. SEDGIS shall use this identification and authentication information in determining the clearance and authorization of all users. SEDGIS shall be capable of associating user identifications with all auditable actions taken by the user.

SEDGIS shall also identify and authenticate the validity of any data (i.e., messages, commands, responses, prompts, etc.) in the system which could be used to circumvent the security of the system.

SEDGIS shall protect authentication data from unauthorized access.

6.7.2 Audit

SEDGIS shall maintain and preserve the integrity of an audit log of all accesses to the data SEDGIS protects. The following actions shall be auditable: use of identification and authentication control mechanisms, introduction of data into user-accessible memory spaces, deletion of data, actions of system administration personnel, any override of human-readable output markings, all events associated with covert channels, and any other security-relevant actions. Additionally, SEDGIS shall maintain a record of the receipt and dispatch of SECRET data for a minimum of 2 years. For each audited action, the log shall indicate the

following: the date and time of the action, the user, the type of action, and the completion or failure of the action. For use of identification and authentication control mechanisms events, the origin of request shall be included in the audit log. For introduction and deletion of data events, the audit log shall identify the data and the security level of the requester.

SEDGIS shall also maintain the capability to monitor security infractions and to take the least necessary counteraction to stop further violations.

6.8 Information Integrity

SEDGIS shall prevent any activity that would alter the response a user receives from a query.

SEDGIS shall not allow modification of E-mail messages once they are submitted, with the exception of deletion by those authorized by the addressee.

SEDGIS shall limit modification of files to the file owner and those designated by the file owner.

6.9 Disposal of Classified Material

SEDGIS shall provide a reliable, auditable mechanism that ensures that classified and/or restricted material can be properly disposed of. This mechanism shall prevent unauthorized reuse of any eliminated or discarded information.

6.10 Trusted Path

The system shall provide peer entity authentication and data origin authentication for communications between the users and the security critical elements when necessary.

7 Assurance

7.1 Operational Assurance

7.1.1 System Architecture

The system security critical elements shall not be subject to external interference or tampering. The system security critical elements shall be of modular design and implementation and shall be of minimum size and complexity.

The system protection mechanisms shall be unbypassable and always invoked.

The system interface shall be completely defined and all protection mechanisms shall be identified. A strict implementation structure shall be in place which enforces the independence of modules.

7.1.2 System Integrity

Diagnostic hardware/software tools shall be used periodically to verify that the security critical elements of the system operate properly.

7.1.3 Covert Channel Analysis

The system shall not permit the compromise of classified or restricted data through the use of covert channels at a rate unacceptable to the system accreditor or DTIC. The system will have documentation indicating the results of the thorough search for covert channels and the estimates, calculations, and reasoning used in determining the expected rate of compromise.

7.1.4 Separation of Function

The system shall provide separate roles with different privileges for the performance of system administration tasks. It shall provide at least two roles, one for daily operational tasks (i.e., operator) and one for configuring and defining the system's and users' security characteristics (i.e., administrator). Personnel in administrator or operator roles shall perform only administrative functions. Administrative personnal shall be limited to the use of authorized software to perform administrative tasks.

7.1.5 Availability/Denial of Service

There are no availability/denial of service security requirements for the SEDGIS system.

7.1.6 Security Failure Analysis

The system shall not allow security to be violated by a mponent failure(s) unacceptable to the system accreditor or DTIC. e system will have documentation indicating the results of the orough testing for potential failures and the estimates, lculations, and reasoning used in determining the expected degree f compromise.

.1.7 Trusted Recovery

The system shall securely recover from failure.

7.2 Life-Cycle Assurance

7.2.1 Configuration Management and Control

The system shall have a configuration management and control system that maintains control of changes to the system configuration and documentation. This shall include the tools necessary to determine the system's current configuration.

8 Documentation

System documentation shall include a system security manual, user security manual, and test documentation.

8.1 System Security Manual

The system security manual shall describe/identify the following attributes of the security system, both at the Gateway and the distributed nodes of the system, at the implementation level:

- All responsibilities, functions and privileges assigned to SEDGIS system administrative and security oversight personnel in securing the SEDGIS facility,
- certification and accreditation procedures,
- how to create, invoke, and maintain system protection mechanisms,
- procedures for generating a new system protection mechanism,
- how to examine and maintain audit data and the audit structures of the various audit events,
- how to change the security characteristics of a user,

- the system protection mechanisms and their associated security critical elements,
- how the system is securely started or re-started,
- how to utilize all security features of the system,
- personnel security,
- acquisition management,
- contingency planning,
- mode of operation determination,
- declassification and release of storage media,
- incident reporting,
- compromise recovery,
- and virus protection.

8.2 User Security Manual

A user manual describing the protection provided by the system protection mechanisms, guidelines on their use, and how they interact with one another, shall be maintained.

8.3 Test Documentation

Test plans, procedures, and results for testing all security enforcement mechanisms shall be maintained and provided to evaluators and other authorized personnel. Test documentation shall show how well the system meets system security specifications and specifically how well the system protects against covert channel exploitation.

APPENDIX C

PRODUCTS

1.0 OPERATING SYSTEMS OR PLATFORMS
- 1.1 TRUSTED XENIX
- 1.2 AT&T 3B2 - SYSTEM V/MLS
- 1.3 XTS-200/STOP
- 1.4 GEMINI COMPUTERS

2.0 SECURE COMMUNICATIONS
- 2.1 KG-84C General Purpose Encryption Equipment
- 2.2 AT&T STU-III Secure Data Device, Model 1900
- 2.3 GE STU-III/LCT 9600 Secure Communications Terminal

1.0 OPERATING SYSTEMS OR PLATFORMS

1.1 TRUSTED XENIX
1.2 AT&T 3B2 - SYSTEM V/MLS
1.3 XTS-200/STOP
1.4 GEMINI COMPUTERS

1.1 TRUSTED XENIX

Introduction

The AT&T 3B2/600G computer is the primary building block of the Standard Multiuser Small Computer Requirements Contract (SMSCRC) system. It is driven by the UNIX® System V Operating System and an array of user-friendly software.

A single computer can support programming, applications, and office automation needs simultaneously. The 3B2/600G can function as a powerful server in a variety of networks so that users can share files, data, and printers for faster communication and improved performance. It can also interact with government-owned mainframes without the need for redundant hardware/terminal emulation.

The 3B2/600G offers flexibility, cost effectiveness, and growth potential. It is reliable and easy to install, use, and maintain.

This catalog provides a concise description of the 3B2/600G computer and its associated equipment, as listed below.

- The basic 3B2/600G cabinet and its contents
- Required system and memory boards and optional boards that mount inside the basic cabinet
- Tape and hard-disk storage devices that mount both inside and outside the basic cabinet
- The console for system administration
- Optional 19-inch unshielded and TEMPEST-certified cabinets for housing the computer.

Each equipment item, where applicable, is identified by its Subcontract Line Item Number (SLIN).

Each equipment description contains a brief general introduction and some or all of the following information:

- Application - Principal use of the device
- Features - Important design/performance characteristics and capabilities
- Specifications - Dimensions, environmental limitations, and power requirements
- Items included - Additional parts and accessories supplied with the main unit
- Requirements - Other conditions, items, and facilities required for normal operation
- Options - A list of optional equipment that can be used with the unit

For additional information or ordering assistance, call our toll-free number: **1-800-DIAL-251.**

Basic 3B2/600G Cabinet

SLIN 0001AA
TEMPEST: SLIN 0001FA

The basic 3B2/600G cabinet provides the housing, wiring, connectors, and utilities for all the components necessary for an operational 3B2/600G computer. It must be equipped with hardware and software listed under Requirements and Options for full service capability. The TEMPEST version must be ordered for use in the TEMPEST-certified 19-inch cabinet (SLIN 0001FC).

Application

- Each SMSCRC system

Features

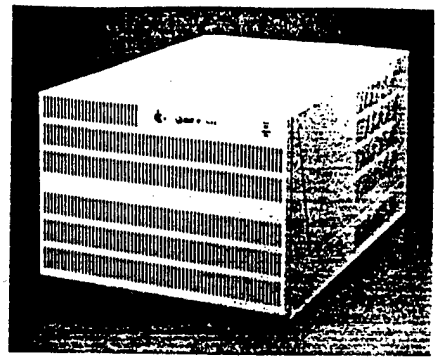
- Compact physical design, aluminum construction, and attractive, unobtrusive appearance
- Hinged front cover with key lock for access to power switch, floppy disk drive, and cartridge tape drive
- Equipped with the following parts and components:
  - Power supply
  - Fans and air filter
  - 720 Kb, 5 1/4-inch floppy disk drive
  - 125 Mb cartridge tape drive for loading, backup, and restore functions
  - Spaces for up to three hard disk drives (ordered separately); used only in non-TEMPEST configurations
  - Power on/standby switch on front panel
  - Power and diagnostics indicators on front panel
  - System reset switch behind front panel
  - Backplane and card cage; access from rear of cabinet
  - Small Computer System Interface (SCSI) host adapter board installed in I/O slot 01 of card cage
- Slots in card cage for the following units (ordered separately):
  - System board
  - Memory boards
  - Multiprocessor enhancement (MPE) feature board
  - Data communications, port, and interface boards
  - Second SCSI host adapter board
- Interface with immediate access storage (IAS) hard disks and tape storage units by way of the SCSI host adapter board and the industry standard SCSI bus
- Maximum disk storage capacity:
  - Non-TEMPEST: 981 Mb internal, 6 Gb external
  - TEMPEST: 0 internal, 3.6 Gb external
- Variety of mounting options:
  - Table top
  - 3B2 expansion cabinet (SLIN 0001DB)
  - TEMPEST cabinet (SLIN 0001FC)
  - Commercial 19-inch cabinet that meets mounting requirements of equipment

Specifications

- 16.9 inches wide x 12.6 inches high x 24.5 inches deep
- 65 to 82 pounds, depending on the components included
- 40 to 100F operating temperature range
- 10F change per 10 minutes or 20F change per hour thermal shock tolerance
- 20% to 80% noncondensing relative humidity
- -250 to 10,000 feet altitude range
- 50 dB(A), or less, acoustic noise
- 120V-60 Hz, 15 amps or 240V-50 Hz, 8 amps nominal input
- Less than 1300 watts power consumption
- +5V, +12V, -12V, and circuit ground outputs
- 3.6V, long-life lithium battery for clock
- 82 pound load tolerance on top of cabinet
- 3000 BTUs/hour heat dissipation
- Compliance of Electromagnetic Interference (EMI) with FCC and VDE Class A requirements in Non-TEMPEST environment and NACSIM 5100A requirements in TEMPEST cabinet environment

Items Included

- SCSI host adapter board installed in I/O slot 01 of the card cage
- Ten blank tape cartridges
- Complete set of documentation



Requirements

- System console (SLIN 0003AA or AB)
- System board (SLIN 0001BC or BE)
- Memory board (SLIN 0002AC or AE)
- Nonremovable hard disk unit (SLIN 0005BA or EA) (non-TEMPEST configuration only) (In a TEMPEST configuration, all hard disk units are removable and mounted external to the basic 3B2/600G cabinet.)
- UNIX operating system (SLIN 0012AA)

Options

- Up to three additional memory boards
- Up to two additional nonremovable hard disk units (non-TEMPEST only)
- Up to two MPE boards (SLIN 0001CA or CC)
- Combination of up to 11 data communications, port, and interface boards in I/O slots:
  - DDN X.25 port 56 Kb/MIL-STD-188-114 boards (SLIN 0004DA)
  - DDN X.25 port RS-232C boards (SLIN 0004DC) (non-TEMPEST only)
  - DDN X.25 port 56 Kb/CCITT V.35 boards (SLIN 0004DE) (non-TEMPEST only)
  - LAN interface boards (SLIN 0004EA)
  - IBM 3270/3274 emulation boards (SLIN 0004EM)
  - Up to 11 EPORTS RS-232C 8-port boards (SLIN 0004AA) (non-TEMPEST only)
  - Up to five fiber expansion module (FXM) RS-232C interface boards (SLIN 0004AC)
  - One additional SCSI host adapter board (SLIN 0001EA)
- Rack-mount hardware kit (SLIN 0001DA) for installation in a 19-inch equipment cabinet

System Board

22 MHz: SLIN 0001BC
24 MHz: SLIN 0001BE

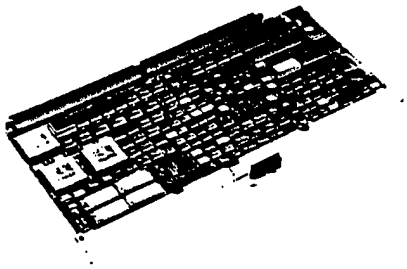
The system board provides central processing and control. It plugs into the double slot in the middle of the card cage.

Application

- Each 3B2/600G computer (Only the 22 MHz board can be used in a TEMPEST configuration.)

Features

- Three main functional areas
  - Central processing unit (CPU)
  - Memory management unit (MMU), which controls information movement to and from memory
  - Math acceleration unit (MAU), which speeds up floating-point calculations
- Two clock speeds available: 22 MHz and 24 MHz
- Very large scale integration (VLSI) devices
- Data paths
  - Internal: 32 bits
  - External: 32-bit address, 32-bit data
- Operations: 8, 16, 32 bits
- Instruction set: IS-25
- CPU instruction cache: 64 by 32 bits
- Fetch controller: 8-byte instruction queue, 32-bit-wide address arithmetic unit (AAU)
- Encoded CPU status outputs: 4
- Dedicated registers (all user accessible)
  - Seven-frame pointer
  - Argument pointer
  - Process status word
  - Stack pointer
  - Process control pointer
  - Interrupt stack pointer
  - Program counter
- Interrupt levels: 15
- Context switching: stack oriented
- Execution privileges: kernel, executive, supervisor, user levels
- Virtual address space: 4 Gb
- Physical address space: 4 Gb
- Memory management: demand paging



- Two RJ45 modular jacks on back plate for RS-232C interface connection with the system console and a peripheral device such as a printer

Specifications

- 15 inches wide x 7.4 inches deep

Requirements

- At least one, or as many as four, memory boards

Options

- Up to two MHz multiprocessor enhancement feature (MPE) boards to increase the system board performance: 18 MHz board with 22 MHz system board; 24 MHz board with 24 MHz system board

Multiprocessor Enhancement Feature Board

18 MHz: SLIN 0001CA
24 MHz: SLIN 0001CC

The optional multiprocessor enhancement (MPE) feature consists of a circuit board and associated software. It provides improvements in system performance. The system board can use up to two MPE feature boards as secondary processing units.

Application

- Any 3B2/600G computer that requires performance beyond the capability of the basic system board

Features

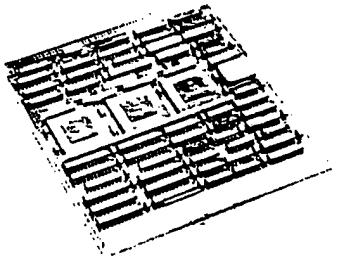
- Three main functional areas
  - Central Processing Unit (CPU)
  - Memory Management Unit (MMU)
  - Math Acceleration Unit (MAU)
- Two clock speeds available: 18 and 24 MHz
- Virtual address cache
  - 4 Kb of memory for instructions
  - 2 Kb of memory for data

Specifications

- 6.5 inches wide x 7.4 inches deep
- Maximum 15 watts power consumption at 5 volts

Items Included

- Feature Manual
- Federal Systems Supplement to feature manual

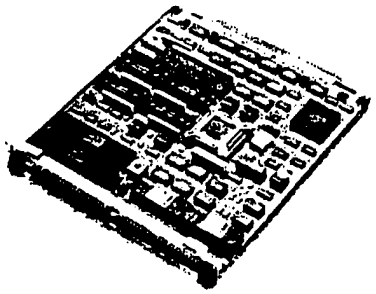


Requirements

- 18 MHz MPE board(s) with 22 MHz system board; mounted in BUB00 and BUB01 slots
- 24 MHz MPE board(s) with 24 MHz system board; mounted in PBUS 0 and PBUS 1 slots

Small Computer System Interface (SCSI) Host Adapter Board

SLIN 0001EA



The SCSI board provides interface between the 3B2 system bus and the SCSI bus, which accesses immediate access storage (IAS) devices. One SCSI board is standard with the 3B2/600G, included with SLIN 0001AA and installed in the card cage. A second SCSI board can be ordered separately for additional storage device interface.

Application

- Each 3B2/600G computer

Features

- Uses one tap on the SCSI bus
- Supports up to seven SCSI peripheral storage devices including the cartridge tape drive (standard card only), hard disk units, and the 9-track tape unit
- SCSI bus connects to storage devices through IAS controllers embedded in each device
- SCSI address switch
- 128 Kb of dynamic RAM (DRAM)
- 32K of erasable programmable ROM (EPROM)
- External direct memory access (DMA)/First In-First Out (FIFO) unit between SCSI and 3B2 I/O bus

Specifications

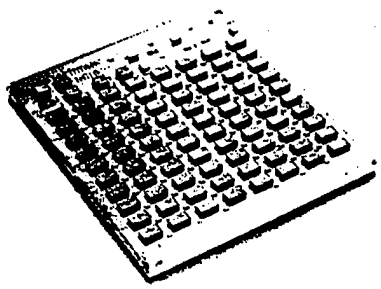
- 6.5 inches wide x 7.4 inches deep
- 10 watts power consumption

Requirements

- For second SCSI: an empty I/O slot in card cage
- SCSI host adapter cable (SLIN 0005RA) for connection from card to first external storage device
- Terminating resistor (part of SLIN 0005RA) to terminate the SCSI bus at the last external storage device
- SCSI daisy-chain cables (SLIN 0005RC) for connections between all external storage devices

Memory Board

4 Mb: SLIN 0002AC
16 Mb: SLIN 0002AE



Up to four memory boards, mounted in card cage slots, provide RAM for the 3B2/600G computer. Memory boards are supplied in modular form so that failure in one module will not deprive the computer of the remaining memory. Failure in the board containing the operating system will "panic" the system, and data will be saved on disks. Memory boards can be installed in the field by either Government or contractor personnel in less than one hour.

Application

- Each 3B2/600G computer

Features

- Available in 4 Mb and 16 Mb sizes
- Surface-mount technology, double-sided
- 4 Mb board uses 256 Kb DRAM chips; 16 Mb board uses 1 Mb DRAM chips
- 32-bit words
- Single- and double-bit error detection and single-bit error correction
- 128 Kb of ROM
- 16 kbps battery backup nonvolatile RAM

Specifications

- 6.5 inches wide x 7.4 inches deep
- 10 watts power consumption

Requirements

- Must be mounted in MEM 0, 1, 2, and 3 slots
- Maximum 64 Mb of memory

System Console

SLIN 0003AA
TEMPEST: SLIN 0003AB

The 3B2/600G system console is an AT&T 605G (Non-TEMPEST) or 605GT (TEMPEST) business communications terminal. This high-quality keyoard/video display unit is a required peripheral used for administration of the 3B2/600G computer. The TEMPEST console is functionally identical to its non-TEMPEST counterpart, but is slightly larger because of its shielding capability.

Application

- Each 3B2/600G computer

Features

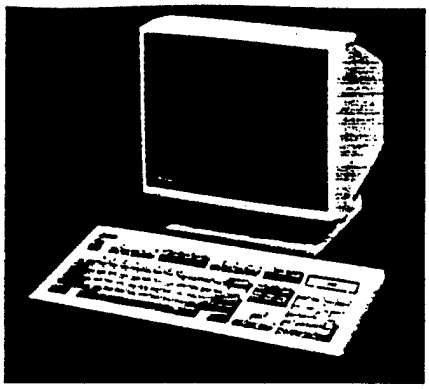
- Asynchronous transmission
- Tilt and swivel monitor
- Detached, low-profile keyboard with 102 keys and 7-foot coiled cord
- Terminal self-test
- Speeds selectable from 300 to 38,400 bps
- Plain English options menu
- Nonvolatile storage for options, screen labels, and strings
- Reverse video screen
- 80 or 132 characters per line
- 27 lines per screen: 24 data, 1 status, and 2 screen label
- Standard RS-232C port for connection to 3B2/600G computer, plus auxiliary RS-232C printer port interface
- Operation modes: interactive, setup, and self-test
- Green phosphor screen

Specifications

- Monitor size:
  - Non-TEMPEST: 12.9 inches wide x 13.3 inches high x 12.8 inches deep
  - TEMPEST: 14.2 inches wide x 14.5 inches high x 15.2 inches deep
- Keyboard size: 18.75 inches wide x 1.5 inches high (2.1 inches tilted) x 7.8 inches deep
- 14-inch (diagonal) viewing screen
- Non-TEMPEST: 22 pounds; TEMPEST: 35 pounds
- 44° to 104°F operating temperature
- 120V-60 Hz, 240V-50 Hz nominal input, switch selectable

Items Included

- Power cable
- User's Guide
- ODS-108 asynchronous filter, RS-232C (TEMPEST only)



Requirements

Non-TEMPEST

- RS-232C cable for connection to 3B2/600G computer: 25-foot RJ45 to DB25 male (SLIN 0010DG) or 50-foot RJ45 to DB25 male (SLIN 0010EG)

TEMPEST

- Cable for connection to coupler on back of TEMPEST cabinet: 15-foot preassembled fiber optic cable (SLIN 0004AP) or fiber optic cable ordered by the foot (SLIN 0010JE) and a set of fiber optic cable terminators (SLIN 0010JG)

Hard Disk Drive Units for Immediate Access Storage

Immediate access storage (IAS) is an SMSCRC high-speed, expandable data storage feature using 5 1/4-inch hard disk units with embedded SCSI controllers. They are available in medium (155 Mb) and large (327 and 608 Mb) capacities.

Up to three 155 or 327 Mb units can be installed internal to the 3B2/600G computer cabinet. In addition, as many as ten (nine, if a 9-track tape drive is used) can be installed external to the 3B2/600G cabinet.

All internal units are nonremovable. They remain in place permanently or until service is required. External units are subdivided into removable and nonremovable. Removable units can be readily pulled from their enclosures for secure storage or transport to another machine.

All external disk units must be housed in Control Data Corporation (CDC) Commer cial Advanced Disk System (CADS) enclosures, also referred to as hard disk cabinets, each of which can hold two units.

In a TEMPEST configuration, all hard disk units must be external, removable, and mounted inside the 19-inch TEMPEST cabinet, SLIN 0001FC.

Application

- Each 3B2/600G computer

Features

- Maximum storage capacity of 7 Gb for one 3B2/600G computer.
- Average seek time of 16.5 milliseconds.
- 512-byte sectors.
- 32-byte data buffer in SCSI controller.
- Removable units certified for 10,000 insertions/removals.
- No tools required for removal of removable units.
- Failure of one disk unit not disabling to any other units.
- UNIX operating system logs failures, reports them to system console, and flags the failed drive as out of service.
- Sealed, ultraclean head/disk/actuator chamber.
- No need for adjustments or preventive maintenance.

Specifications

- Approximately 8 pounds
- 5.75 inches wide x 3.5 inches high x 8 inches (internal) or 10.5 inches (external) deep
- Less than 45 dB(A) acoustic noise

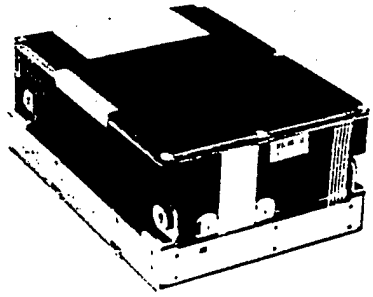
Requirements

- One or more CADS enclosures for external hard disk units. Each enclosure can hold one or two units. The SLIN 0005PA stand-alone enclosure is required for non-cabinet applications.

SLIN 0005AA–SLIN 0005JA

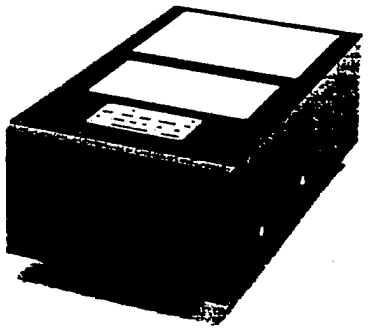
155 Mb: SLIN 0005EA
300 Mb: SLIN 0005BA
Internal/Nonremovable

These are the only hard disk units that can be installed inside the 3B2/600G cabinet. The medium capacity disk (SLIN 0005EA) is a Wren™ III model. The large capacity disk (SLIN 0005BA) is a Wren IV with an actual formatted storage space of 327 Mb.



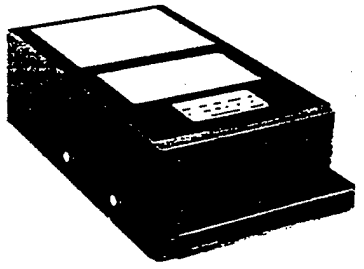
155 Mb: SLIN 0005EC
300 Mb: SLIN 0005BC
External/Nonremovable

These units are designed for permanent installation in CADS enclosures (SLIN 0005PA or QA). The medium capacity disk (SLIN 0005EC) is a 155 Mb Wren III model. The large capacity disk (SLIN 0005BC) is a Wren IV with an actual formatted storage space of 327 Mb. (An acceptable alternative to an external nonremovable unit is a removable unit of the desired capacity.)



155 Mb: SLIN 0005AB
155 Mb (TEMPEST): SLIN 0005JA
300 Mb: SLIN 0005AA
550 Mb (TEMPEST): SLIN 0005HA
External/Removable

These units are designed for insertion in CADS enclosures. They are Wren models housed in cases with handles and designated as removable transportable memory modules (RTMMs). The medium capacity units (SLINs 0005AB and JA) are CDC RTMM-155s (Wren III). TEMPEST and non-TEMPEST models are completely interchangeable. The large capacity SLINs 0005AA and HA are CDC RTMM-300 (Wren IV) and RTMM-550 (Wren V) models, respectively; their actual formatted capacities are 327 Mb and 608 Mb. The TEMPEST model can be used in non-TEMPEST configurations.

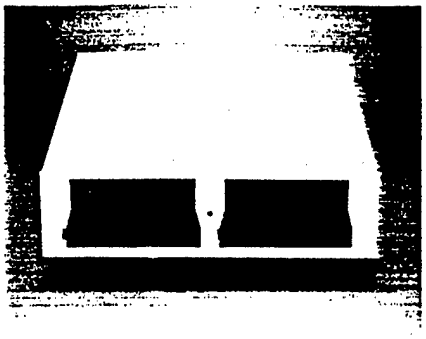


The SLIN 0005QA rack-mount enclosure is required for all installations in 19-inch cabinets.

- A second SCSI host adapter board in the 3B2/600G cabinet card cage if the number of SCSI units exceeds the capacity of the standard SCSI board (six hard disk units or five hard disk units and a 9-track tape unit).
- One SCSI host adapter cable (SLIN 0005RA) to connect the 3B2/600G cabinet to the first external unit on the SCSI bus
- One SCSI [illegible] (SLIN 0005RC) [illegible] unit on the SCSI [illegible]
- One [illegible] (SLIN 0005R[illegible]) [illegible] SCSI bus at the [illegible] 9-track tape drive [illegible] SCSI bus. It should [illegible]

CADS Enclosure (Hard Disk Cabinet)

Stand-Alone: SLIN 0005PA
Rack-Mount: SLIN 0005QA



The Commercial Advanced Disk System (CADS) enclosure is manufactured by Control Data Corporation to house its RTMM hard disk units. It can also be used for external nonremovable hard disk units.

Application

- SMSCRC systems with hard disk units mounted external to the basic 3B2/600G computer cabinet

Features

- Capacity for one or two hard disk units
- SCSI connections, power, and cooling

Specifications

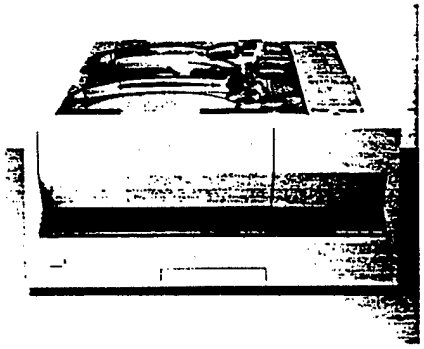
- 16.8 inches wide x 5.1 inches high x 22 inches deep
- Approximately 27 pounds (without disk units)
- 50° to 105° operating temperature
- 8% to 80% noncondensing relative humidity
- 115V-60 Hz or 230V-50 Hz nominal input, switchable
- 88 watts power consumption with two disk units
- 45 dB(A) acoustic noise with two disk units
- 300 BTUs/hour heat dissipation with two disk units

Requirements

- Stand-alone model for table-top use
- Rack-mount model for mounting in a 19-inch cabinet (such as SLIN 0001DB 3B2 expansion cabinet or SLIN 0001FC TEMPEST cabinet)

Nine-Track Magnetic Tape Unit

Stand-Alone: SLIN 0006AA
Rack-Mount: SLIN 0006AC



The optional 9-track tape unit is a model HP88780A manufactured by Hewlett-Packard Corporation. It is an autoloading, horizontally mounted, 1/2-inch, reel-to-reel machine that provides high-speed backup and restore capabilities to the 3B2/600G computer. The tape unit, like the hard disk units, operates off the SCSI bus.

Application

- Any 3B2/600G computer that requires a high-speed, high-capacity tape facility in addition to the standard cartridge tape unit

Features

- Read/write speed of 125 inches per second (ips)
- Rewind speed of 320 ips (rewinds a 2400-foot reel in 90 seconds)
- Handles both 6250 characters-per-inch (cpi) group-coded recording and 1600 cpi phase-encoded ANSI formats
- 512 Kb internal buffer
- Error detection and correction
- Autoload feature centers any standard size reel from 6 to 10.5 inches, locks the reel, and threads the tape
- Autoload success rate of 98%
- No field adjustments or periodic maintenance other than cleaning tape path and head
- Board-level diagnostics
- Control panel with operation keys, status indicators, and error message display

Specifications

- 19 inches wide x 8.75 inches high x 26.5 inches deep
- 85 pounds
- 59° to 90°F operating temperature
- 20% to 80% noncondensing relative humidity
- 120V-60 Hz or 240V-50 Hz nominal input, switchable
- 250 watts maximum power consumption
- 54 dB(A) maximum acoustic noise

Items Included

- Ten blank tapes
- User's Guide

Requirements

- Cable and terminating resistor (see section on SCSI Host Adapter Board)
- SLIN 0001DC, which includes slides and brackets for converting a SLIN 0006AA stand-alone tape unit to a rack-mount unit equivalent to SLIN 0006AC; required only when mounting an existing SLIN 0006AA in a 19-inch equipment cabinet
- Last unit on SCSI bus (after hard disk units)
- Rack-mount unit (SLIN 0006AC) in TEMPEST configuration

3B2 Expansion Cabinet

This AT&T 19-inch industry standard cabinet is a compact, protective, and attractive housing for certain components of SMSCRC equipment.

Application

- Installations where cabinet enclosure of one or two 3B2/600G computers and associated hard disk and magnetic tape equipment is desirable for space-saving, accessibility, and aesthetic reasons.

Features

- Steel construction
- Off-white color
- Removable front and rear doors with air vents
- Casters on all four corners
- Retractable anti-tip leg on front of cabinet
- Slide mounting available separately for 3B2/600G and 9-track tape unit
- Cooling and air circulation provided by the equipment mounted in the cabinet

SLIN 0001DB

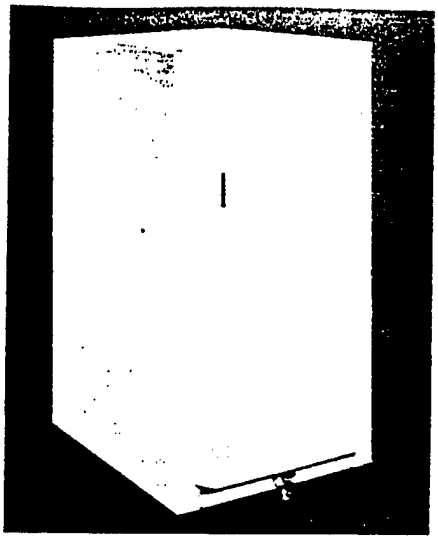
- Standard mounting arrangement: 3B2/600G computer at the bottom, hard disk cabinet(s) in the middle, and 9-track tape unit at the top
- Easy accessibility for maintenance
- Cable entry through lower rear
- Filler panels for covering unused spaces

Specifications

- 24.75 inches wide x 48.5 inches high x 33 inches deep
- 42 inches of vertical mounting space
- Mounting height expressed in units of 1.75 inches each, for a total of 24 units. Equipment unit requirements:
  - 3B2/600G computer, 9 units
  - Tape unit, 5 units
  - Hard disk cabinet, 3 units
  - Filler panel, 1 unit
- Approximately 220 pounds (empty)

Requirements

- Mounting hardware kit (SLIN 0001DA) for 3B2/600G computer
- Filler panels (SLIN 0001DD) for all unused spaces to maintain constant flow of cooling air



- For hard disk units installed external to the 3B2/600G: rack-mount hard disk cabinets (SLIN 0005QA)
- For 9-track tape unit: rack-mount unit (SLIN 0006AC) or existing stand-alone unit (SLIN 0006AA) equipped with a rack-mount kit (SLIN 0001DC)

TEMPEST Expansion Cabinet

This 19-inch cabinet provides a compact, attractive, TEMPEST-certified, shielded housing for certain SMSCRC equipment.

Application

- Installations where electronic shielding of a 3B2/600G computer, up to three hard disk cabinets (CADS enclosures), a 9-track tape unit, and up to three FXMs is desirable for security reasons

Features

- Full TEMPEST shielding
- Fiber optic connections to external equipment
- Front and rear doors
- Mounting facilities for FXMs on inner side of rear door
- 120V-60 Hz or 240V-50 Hz power filter with six outlets and shielded 6-foot power cord
- Cooling fans
- Casters on all four corners

SLIN 0001FC

- Standard mounting arrangement: 3B2/600G computer on the bottom, hard disk cabinets in the middle, and 9-track tape units at the top: FXMs on inner side of rear door

Specifications

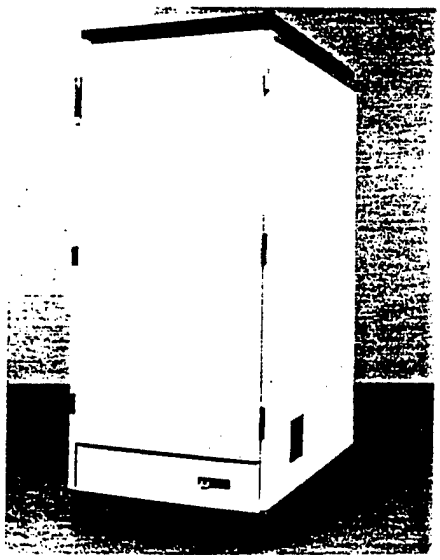
- 24 inches wide x 52 inches high x 36 inches deep
- Approximately 200 pounds (empty)

Items Included

- 16 SMA couplers
- RS-232C cable
- RJ45 to DB25M adapter
- ODS-107 asynchronous filter, RS-232C
- 3-foot fiber optic cable

Requirements

- Mounting hardware kit (SLIN 0001DA) for 3B2/600G computer
- For hard disk units installed external to the 3B2/600G: rack-mount hard disk cabinets (SLIN 0005QA)



- For 9-track tape unit: rack-mount unit (SLIN 0006AC) or existing stand-alone unit (SLIN 0006AA) equipped with a rack-mount kit (SLIN 0001DC)

Trademarks

UNIX is a registered trademark of AT&T.
Wren is a trademark of Control Data Corporation.

Introduction

This catalog describes the array of software products available through the Standard Multiuser Small Computer Requirements Contract (SMSCRC). For your ordering convenience, each item is identified by Subcontract Line Item Number (SLIN).

You'll find product descriptions organized as follows:

- GOE Integration Software, SLIN 0004KA through SLIN 0004QA
- Operating System, SLIN 0012AA through SLIN 0012LA
- Secure Operating System, SLIN 0012HA through SLIN 0012KA
- RDBMS Conversion Software, SLIN 0012LA
- Data Base Software, SLIN 0013AA through SLIN 0013CA
- Communications Software, SLIN 0015AA through SLIN 0015DA
- Compilers, SLIN 0016AA through SLIN 0016GA
- Office Automation, SLIN 0017AA through SLIN 0017RA
- Bar Code Software, SLIN 0018AA

Each software package has been tested, certified, and approved for procurement by the U.S. Government's SMSCRC Program Office.

If you need additional information or would like to place an order, simply call our toll free number: **1-800-DIAL-251.**

PC-Interface

SLIN 0004KA

PC-Interface™ Personal Computer Software

This software package includes components for the PC and host computers and executes over IEEE 802.3 local area networks (LANs) running TCP/IP.

Applications:

- PC-established directories on host
- Remote printing
- Increased PC functionality

Features:

- Transparent use of file storage and printers located on the host
- Execution of noninteractive UNIX® system processes from the PC
- Administration of network facilities
- Ability to simultaneously access multiple hosts on the SMSCRC network

Items Included:

- PC-Interface/SMB User's Guide

Requirements:

- 353 Kb shared memory on host
- 3BNET present on host
- EtherLink® card present in PC (SLIN 004JA)
- Defense Data Network (DDN) (SLIN 0015AA)
- NETBIOS interface software (SLIN 0015CA)

Distributed SQL Interface

SLIN 0004LA

ACCELL/CP®

ACCELL/CP provides the capability for off-loading, intensive screen handling, and keyboard editing from the host to the faster terminal or PC. Therefore, the host can handle data management and application processing at a much faster rate, improving performance.

Applications:

Ideal for a system having heavy loads of screen editing and report writing.

Features:

- Improved host performance
- Host will support more users
- Decreased I/O traffic
- Window management
- One-button control to switch between DOS® and UNIX system PCs

Items Included:

- ACCELL/CP software
- Cooperative applications
- ACCELL/CP cooperative processing application, Issue 2

Requirements:

- 256K memory
- RS-232C serial port or IEEE 802.3 running TCP/IP
- ACCELL® installed (SLIN 0013CA)
- Relational Data Base Management System (RDBMS) (SLIN 0013AA)

Database Extraction

SLIN 0004MA

Multiplex™

This software package allows the PC workstation user to extract data from the UNIFY® data base of the AT&T 3B2/600G via RS-232C connections or IEEE 802.3 LANs running TCP/IP.

Applications:

Effective where it is required that the PC user extract data from the UNIFY data base.

Features:

- Two components, one for PC and one for 3B2/600G host
- Access to UNIFY through a simple menu interface
- Automatic formulation of Structured Query Language (SQL™) for UNIFY data bases
- Ability to browse the contents of the data base on the PC screen, select data, and move it to the PC
- Automatic reformatting of data for compatibility with PC software packages (including Lotus®, dBASE II® and III®, Framework™, Multiplan®, WordStar®, and Symphony™)

Items Included:

- Multiplex software
- Multiplex User's Manual

Requirements:

- RS-232C or IEEE 802.3
- Host must contain one of the following SLINs: 0013AA, 0013BA, 0017SA, 0017TA

Remote File Sharing

SLIN 0004NA

AT&T Remote File Sharing Utility

Remote File Sharing provides an expanded set of files, peripherals, and software to PCs or terminals connected to multiple 3B2/600G computers. The PCs can be connected by direct wire or by an IEEE 802.3 network running TCP/IP.

The Remote File Sharing concept is similar to that of PC-Interface, but will allow the transparent sharing of resources *between* 3B2/600G computers. For example, users can set up a file system on Computer A and remotely access it from Computer B. In turn, users of Computer B can access the files as if they were local resources.

Applications:

- Ideal where resources must be shared
- Applicable where quick and easy access to information such as corporate data bases is required

Features:

- Expanded PC capabilities
- Easy access to information
- Reduced peripheral costs

Items Included:

- Remote File Sharing software
- AT&T 3B2 Computer Remote File Sharing Utilities, Release 1.2 Release Notes
- Federal Systems Supplement to AT&T 3B2 Computer Remote File Sharing Utilities, Release 1.2 Release Notes
- Federal Systems Supplement to AT&T 3B2 Remote File Sharing Utilities, Release 1.2 Update to the System Administration Guide

Requirements:

- NI board or DDN board
- TCP/IP software (SLIN 0015AA) to interconnect the various 3B2/600Gs

Document Conversion Software

SLIN 0004PA

KEYpak™

KEYpak, a software product from Keyword Office Technologies, allows users to convert a document from one word processing software package to another while retaining the original format.

Applications:

Ideal where transmitting/receiving documents to/from other word processing systems is required.

Features:

Supports 25 word processing formats:

- ASCII (Intelligent)
- COM.FILE (KSIF)
- Convergent/DEF
- DECdx®
- DisplayWrite 2, 3 and 4™
- IBM® DCA-FFT
- IBM DCA-RFT
- Microsoft Word® (MAC)
- Microsoft Word (PC)
- MultiMate®
- MultiMate Advantage
- Navy/DIF
- NBI OASys Archive
- OfficeWriter™
- PrimeWord
- Q_ONE™ (UNIX)
- Samna Word III™
- Wang OIS/VS®
- Wang PC®
- Wang WITA®
- WordERA
- WordMARC®
- WordPerfect®
- WordStar®
- Xerox Writer II/III®

Items Included:

- Conversion software
- KEYpack System Manager's Guide

Requirements:

- 5 Mb disk storage

Software For Access To Multiple Remote Resources

SLIN 0004QA

ASCENT™

ASCENT software, a UNIX system-based application from Control Data Corporation, provides a simple way to routinely upload and download data from a number of host computers (IBM® and others) located on a variety of networks.

Scripts must be written to perform desired tasks but, once in place, can be used easily by even the most inexperienced users to perform complicated tasks. (CLIN 0027 on the SMSCRC can be used to order support for script preparation.)

Applications:

Upload and download files to and from networked hosts.

Features:

- Resides on the 3B2/600G computer.
- If a network is unavailable, system will automatically seek another path until connection is made.

Items Included:

- ASCENT software
- ASCENT User's Guide
- ASCENT Programmer Guide
- ASCENT Installation and Administrator's Guide
- ASCENT Mail User's Guide

Requirements:

- DDN, IEEE 802.3, TYMNET or direct dialing must be available
- C Compiler (SLIN 0016FA)
- Software Generation Utilities (SLIN 0016GA)

Operating Systems and Utilities

SLIN 0012AA

AT&T UNIX System V, Release 3.2.2

AT&T's UNIX System V, Release 3.2.2 is the cornerstone for SMSCRC's open architecture. Release 3.2.2 provides more flexible directory and file administration than earlier UNIX system releases. It includes enhanced communications and networking capabilities and powerful interprocess communications. In addition, it fully supports the hardware features of AT&T's 3B2/600G computer.

The improved computer networking capabilities of Release 3.2.2 allow transparent access to remote data and resources. At the department level, peripherals, software, and data can be shared transparently among many different types of equipment. In addition, mainframe, department, and workstation levels can interweave and exchange information in a seamless manner.

A Prelude™ Screen Shell from VenturCom is bundled with UNIX System V, Release 3.2.2. It serves as the backbone for a user-friendly interface to underlying SMSCRC applications, utilities, and commands.

Applications:

- Used as operating system where system flexibility and open architecture are required
- Expands networking capabilities

Features:

- Security enhancements
- Character-based, multiwindow, user interface to simplify the system for novice users
- Improved line printer spooling utilities
- Improved demand paging capabilities for better performance and more efficient use of memory
- Improved file backup and restore
- International capabilities including 8-bit code sets, foreign language terminals, and alternate date/time conventions
- 2K file system support

Items Included:

- AT&T 3B2/600G diagnostic software
- Assist utilities
- Basic networking utilities
- Directory and file management utilities
- User environment utilities
- Editing utilities
- Enhanced ports (EPORTS) utilities
- Essential utilities (CORE)
- Extended core update utilities
- File translation utilities
- Graphics utilities
- Help utilities
- Interprocess communication utilities
- Line printer spooling utilities
- Manual (MAN) command
- Terminal information utilities
- System header files
- Terminal filter utilities
- Performance measurement utilities
- Screen management utility
- Tape dump utilities
- SCSI disk utilities
- SCSI host adapter utilities
- System administration utilities
- Spell utilities
- System accounting utilities
- Prelude screen shell generator
- User-friendly interface
- Documenter's Workbench® software
- Networking support utilities
- PC disk
- SCSI cartridge tape utilities
- TPLUS™ and TROFF interface software
- UNIX System V User's Guide
- AT&T UNIX System V ASSIST Software User's Guide
- AT&T UNIX System V ASSIST Software Development Tools Guide
- AT&T 3B2 computer, UNIX System V User's and Administrator's Reference Manual(s)
- AT&T 3B2 Computer Networking Support Utilities Release 1.2 Release Notes
- AT&T 3B2 computer, UNIX System V, Release 3.2, System Administrator's Guide
- User-Friendly Interface User's Manual
- CT-Mail™ Conversion User's Manual
- Federal Systems Supplement to AT&T 3B2 Computer Networking Support Utilities
- Federal Systems Update for AT&T 3B2 Computer, UNIX System V Reference Manual
- Federal Systems Supplement to AT&T 3B2 computer, UNIX System V System Administrator's Guide
- Federal Systems Supplement to UNIX System V ASSIST Software User's Guide
- Update for AT&T 3B2 computer, UNIX System V User's and System Administrator's Reference Manual
- Federal Systems TROFF/TPLUS Laser Typesetting Technical Discussion
- Federal Systems TROFF/TPLUS Laser Typesetting User's Guide
- Prelude Screen Shell Developer's Guide
- AT&T 3B2 computer, UNIX System V Release 3.2.2 Release Notes
- Federal Systems Utilities Release 1.2.3 Release Notes

Requirements:

- 4 Mb RAM
- 30.6 Mb disk storage

Sanitization Software

SLIN 0012CA

AT&T Sanitization Utilities

AT&T sanitization software allows users to declassify a system that has been used for classified data, or to prepare a system for classified operation by removing all data from disks, tapes, and memory. Verification capabilities are included.

Applications:

Used where classified data may be required on system part time.

Features:

- Utility for overwriting 3B2/600G main memory
- Utility for overwriting removable and nonremovable disk storage
- Utility for overwriting magnetic tape

Items Included:

- Sanitization software
- System Sanitization User's Manual

Portable Operating System (P1003)

SLIN 0012DA

This will replace SLIN 0012AA as the UNIX system standard set by IEEE.

Trusted Computing Base

C2-Level, SLIN 0012HA
B1- Level, SLIN 0012JA

AT&T System V/MLS

AT&T System V/MLS provides a secure, UNIX System V-compatible computing environment for B1- or C2-level needs, and it does so *without* sacrificing performance or usability. In even the worst of cases, performance is degraded by less than five percent.

System V/MLS was certified by the National Computer Security Center in September, 1989, making it the *only* System V-compatible product to achieve this major milestone. It is highly resistant to computer viruses, Trojan Horse programs, and other attacks by hackers.

The site administrator can operate System V/MLS in either C2 or B1 mode. To operate in C2, all users are cleared to *one* security level. B1 mode allows the system administrator to partition data further, setting up multiple classification levels or categories and clearing individuals to operate at these new levels. This approach allows users to operate with multiple security levels and to restrict access to each grouping of data.

Whether the C2- or B1-level is used, System V/MLS will protect the system from tampering by establishing a system-level label for all system components. Only the system administrator is cleared to operate at the system level. As a result, the trusted computing base is always protected, regardless of the operating level selected.

Applications:

Used on systems where classified data will reside.

Features:

- Explicit security labels for processes, files, directories, and other important entities
- Mandatory access control policy to protect sensitive objects from unauthorized access
- Automatic audit of security-critical operations with a record stored in a protected audit trail
- Automatic password generator to ensure that easily guessed passwords are not chosen

Items Included:

- Trusted computing base, operating system, and utilities
- System V/MLS Trusted Facility Manual
- System V/MLS User's Guide and Reference Manual

Requirements:

- 4 Mb RAM
- 10 Mb disk storage

Operating System Upgrade To Trusted Computing Base

SLIN 0012KA

AT&T System V/MLS

AT&T System V/MLS provides users with the capability to upgrade existing UNIX system installations to a B1 or C2 secure system.

This upgrade provides the same effective level of security as the Trusted Computing Bases B1 and C2.

Applications:

Provides upgrade to the UNIX system when more security is needed.

Features:

- Explicit security labels for processes, files, directories, and other important entities
- Mandatory access control policy to protect sensitive objects from unauthorized access
- Automatic audit of security-critical operations with a record stored in a protected audit trail
- Automatic password generator to ensure that easily guessed passwords are not chosen

Items Included:

- Operating system upgrade to trusted computing base
- System V/MLS Trusted Facility Manual
- System V/MLS User's Guide and Reference Manual

Requirements:

- 4 Mb RAM
- 10 Mb disk storage

RDBMS Conversion Utility

SLIN 0012LA

AT&T RDBMS Conversion Utility

The AT&T RDBMS Conversion Utility is designed to convert data from the reQuest™ Data Base Management System to the UNIFY RDBMS.

Applications:

Combines a data dictionary report file and associated data files as input to build a UNIFY 2000 script file and dbld load file.

Features:

- Ability to build UNIFY 2000 schema script file from a reQuest DBMS data dictionary report file.
- Ability to build UNIFY 2000 dbld specification file and load file from reQuest DBMS data file. (dbld utility allows bulk loading or updating of rows in an existing UNIFY 2000 data base table.)
- Ability to review conversion messages recorded by the RDBMS Conversion Utility.

Items Included:

- RDBMS Conversion Utility
- AT&T RDBMS Conversion Guide

Requirements:

- A data dictionary report file and data files from a reQuest DBMS Version 4.0 data base (must be resident on your SMSCRC 3B2/600G computer)

Relational Data Base Management System

SLIN 0013AA

UNIFY 2000

The UNIFY 2000 Relational Data Base Management System is designed for large, sophisticated applications involving transaction processing with 100 percent uptime requirements.

It provides support for all primary access methods: direct, B-tree, hashing, link, and sequential. It also provides excellent tools for software developers.

Applications:

Used when large amounts of data must be stored and manipulated for output.

Features:

- On-line backup to run an application while copying data base onto backup media
- Dynamic Data Definition Language (DDL) for on-line modification of data base design without halting operation
- Automatic recovery in the event of system failure
- ANSI-compliant Structured Query Language (SQL)
- Embedded SQL for C, COBOL, and Ada® programming languages
- Interactive report writer (RPT®) for development of multilevel tabular reports with English language commands

Items Included:

- Relational Data Base Management System
- RDBMS Developer's Reference Manual
- RDBMS User's Manual
- RDBMS RHLI Programming Manual
- RHLI Quick Reference Guide
- Embedded SQL/A Quick Reference Guide
- Interactive SQL/A Quick Reference Guide
- Addendum to UNIFY 2000 Release Notes for Release 1.0.3

Requirements:

- 512 Kb RAM
- 2 Mb disk storage

RDBMS Runtime

SLIN 0013BA

This is the runtime only version of SLIN 0013AA. It can only run data bases and applications previously developed and compiled using SLIN 0013AA. The data base structure or applications programs *cannot* be changed with this package.

Items Included:

- UNIFY Runtime Software
- UNIFY Runtime Installation and Release Notes
- Addendum to UNIFY 2000 Release Notes for Release 1.0.3

Fourth Generation Language (4GL)

SLIN 00013CA

ACCELL

ACCELL is a development system that integrates an application generator and a fourth generation language with the UNIFY RDBMS.

Applications:

Used when high developer productivity is a requirement.

Features:

- Updates screen layouts without recompiling
- Window manager
- Unlimited number of overlapping windows
- Zoom view
- Fill-in-the-blank forms
- On-line help
- Automatic compilation and merging of ACCELL/Language with ACCELL/Generator information
- Extensive nonprocedural capabilities

Items Included:

- Fourth generation language software
- ACCELL Developer's Environment Reference Manual
- ACCELL/4GL Quick Reference Guide
- Addendum to UNIFY 2000 Release Notes for Release 1.0.3

Requirements:

- 4 Mb RAM
- 35 Mb hard disk
- Relational Data Base Management System (SLIN 0013AA)
- C Compiler (SLIN 0016FA)
- Software Generation Utilities (SLIN 0016GA)

TCP/IP WIN/3B

SLIN 0015AA

AT&T Enhanced TCP/IP WIN®/3B Software with STREAMS

AT&T's enhanced TCP/IP WIN/3B software supports three remote login utilities: telnet, rlogin, and remsh. These utilities allow users to log in and use host computers as if they were directly connected to the terminal.

AT&T's TCP/IP WIN/3B is supplemented by a STREAMS network support utility, providing a uniform method for imple-menting multiple network protocols. STREAMS broadens the access to network services — at substantial cost savings.

This is the high-level software used to drive the DDN boards and the NI (EtherNet™) boards. While it is called "DDN software" in the Contract B-Tables, this is somewhat misleading, as it includes, in addition to the TCP/IP software, the low-level device drives for both the DDN and the NI boards.

Applications:

Applicable where shared facilities are required; also where multiple network protocols are present.

Features:

- **telnet.** Uses Department of Defense Transmission Control Protocol (TCP) for connection to any host that supports this standard, regardless of the operating system it uses.
- **rlogin.** Provides automatic login to remote hosts without prompting for login name, password, or terminal type. Works between hosts running the UNIX operating system.
- **telnet and rlogin virtual terminal.** Appears directly connected to the remote host, providing full user capabilities and privileges until the connection is broken and control is returned to the local operating environment.
- **remsh.** Allows quick login and execution of a single command on a remote host and automatic return to the local host computer. Works between remote hosts which run the UNIX or EUNICE operating systems.

Items Included:

- Defense Data Network Communications Software
- UNIX System V STREAMS Primer
- Federal Systems Supplement to UNIX System V STREAMS Primer
- AT&T Enhanced TCP/IP WIN/3B Installation and Administration Guide
- Release 3.0 Release Notes
- AT&T Enhanced TCP/IP WIN/3B User's Guide
- AT&T Enhanced TCP/IP WIN/3B Reference Manual

Requirements:

- 3600 Kb "/USR" and 800 Kb "/" free disk space
- NI board or DDN board (SLIN 0015AA)

Source Code For DDN Communications Software

SLIN 0015BA

This software allows the DDN (SLIN 0015AA) source code to be compiled/assembled on the user's 3B2/600G computer. Approval from the SMSCRC Program Office at Gunter AFB is required prior to ordering this item.

NETBIOS Interface

SLIN 0015CA

PC-Interface 3B2 Computer Host Software, Version 1.0, Locus Computing Corporation

AT&T provides both a robust IEEE 802.3 local area network (LAN) interface and IBM PC-compatible NETBIOS software for the AT&T 3B2/600G computer.

The IEEE 802.3 10base5 interface (SLIN 0004AE) is provided by an intelligent, microprocessor-based controller which occupies one card slot on the 3B2/600G's enhanced I/O bus.

PC-Interface 3B2 Computer Host Software provides a full-featured NETBIOS interface between IBM PC-compatible personal computers and the 3B2/600G. To maximize the capabilities of this interface, users will need the corresponding PC-Interface software, Release 1.0 (SLIN 0004AJ2) and the TRW IEEE 802.3/NETBIOS interface card (SLIN 0004AJ3) for networked IBM PC-compatible personal computers.

Applications:

Ideal where files and printers must be shared.

Features:

- Transparent file and printer sharing
- Terminal emulation
- UNIX system mail
- UNIX system process execution

Items Included:

- NETBIOS Interface Software
- PC Interface/SMB Administrator's Guide
- PC Interface/SMB Command Summary

Requirement:

- IEEE 802.3 10base5 interface card on host (SLIN 0004AE)
- PC Interface Software Release 3.0
- TRW IEEE 802.3/Netbios interface card on PC
- TCP/IP on the host
- Defense Data Network (DDN) (SLIN 0015AA)

IBM 3270 Emulator

SLIN 0015DA

AT&T SNA/3270 Emulator+, Release 3.0

The AT&T 3270 Emulator+, Release 3.0, supports interactive communications between ASCII terminals connected to AT&T 3B2 computers and remote IBM mainframes. The emulator functions as an IBM 3274-51C cluster controller, an IBM 3278/9 information display station, and an IBM 3287 printer.

Applications:

Where communications are required between ASCII terminals connected to 3B2/600G and IBM mainframes.

Features:

- High Level Language Application Program Interface (HLLAPI). Emulates an operator at a terminal, allowing local applications to interact with multiple host applications. Allows migration from IBM 3279 PC HLLAPI programs to the multiuser environment of the AT&T 3B2/600G computer.
- ESCORT. Provides interactive, tutorial, and script interfaces between the operator and applications. In the interactive mode users can access applications as if they were entering data on an IBM 3278 or DEC VT 100 terminal.

Items Included:

- AT&T 3270 Emulator+ User's and Administrator's Guides

Requirements:

- 512 Kb RAM
- 20 Mb hard disk
- IBM 3270/3274 emulation port card (SLIN 0004EM)

COBOL Compiler

SLIN 0016AA

LPI-COBOL™ (from Language Processors, Inc.)

LPI's COBOL is a full implementation of ANSI and COBOL 85 and 74, validated at a high level. To protect your software development investment, it is fully X/OPEN-compliant.

LPI's COBOL is also source-code compatible with RM/COBOL, allowing users to transport applications to the LPI environment without modification. Similar extensions have been added for Micro Focus LEVEL II COBOL™, IBM/370 and the earlier COBOL-68 standard.

Features:

- Can be debugged with LPI-DEBUG™ Since all interactions with the debugger use COBOL terms, users will not need to know the machine language of the host computer.
- Allows communication between subprograms written in COBOL or any other LPI language.
- Produces error messages in complete sentences. Programming errors are clearly identified, and instructions are provided on how to correct them.
- Makes full use of the LPI optimization facilities.

Items Included:

- COBOL Compiler Software
- LPI-COBOL User's Guide
- LPI-COBOL Language Reference Manual
- LPI-COBOL Quick Reference Guide
- LPI-COBOL Release Notes

Requirements:

- 128 Kb RAM
- 740 Kb disk space
- Software Generation Utilities (SLIN 0016GA)

FORTRAN Compiler

SLIN 0016BA

LPI-FORTRAN™ (from Language Processors, Inc.)

LPI's FORTRAN is an implementation of ANSI and MIL-STD-1753 compatible FORTRAN-77. To protect user investment, it is fully X/OPEN-compliant.

LPI's FORTRAN includes key extensions for compatibility with VAX™ FORTRAN and MIL-STD-1753. These extensions make it easier to transport applications from large mainframes to the SMSCRC's AT&T 3B2/600G host processor.

Features:

- Can be debugged with LPI-DEBUG™ Since all interactions are in FORTRAN, users will not need to know the machine language of the host computer.
- Allows communication between subprograms written in FORTRAN or any other LPI language.
- Produces error messages in complete sentences. Programming errors are clearly identified, and instructions are provided on how to correct them.
- Makes full use of the LPI optimization facilities.

Items Included:

- FORTRAN Compiler Software
- LPI-FORTRAN User's Guide
- LPI-FORTRAN Language Reference Manual
- LPI-FORTRAN Quick Reference Guide
- LPI-FORTRAN Release Notes

Requirements:

- 2 Mb RAM
- 8,270 blocks free disk space which includes 2,915 and 5,355 for the user
- Math Application Unit
- Software Generation Utilities (SLIN 0016GA)

ADA Compiler

SLIN 0016CA

VERDIX Ada Development System for the AT&T 3B Computer Family

The VERDIX Ada Development System (VADS) for the AT&T 3B computer family is centered on a high-performance, production-quality compiler that fully complies with ANSI/MIL-STD-1815A. It is designed to provide a production environment that maximizes both compilation speed and runtime efficiency.

The VERDIX Ada Compiler is exceptionally user-friendly, featuring innovative, syntactic, error-recovery techniques. It generates a concise description of the error and directs the user to a specific subsection in the Ada Reference Manual for a more detailed explanation.

The compiler generates native code for the AT&T 3B computer family. An optimizer boosts execution performance.

Applications:

Provides a production-quality system intended for large-scale development of both application and systems software.

Features:

- Screen-oriented debugger
- Library maintenance utilities
- Programming tools
- Runtime system

Items Included:

- Ada Compiler Software
- VERDIX - Ada Quick Reference Guide
- VERDIX - Ada User's Guide

Requirements:

- 25,000 blocks disk space
- Software Generation Utilities (SLIN 0016GA)

PASCAL Compiler

SLIN 0016DA

LPI-PASCAL™ (from Language Processors, Inc.)

LPI's PASCAL fully implements ANSI and ISO standards. It also includes popular extensions from other PASCAL dialects.

Features:

- Makes full use of LPI multiple optimization levels.
- Can be debugged with LPI-DEBUG. Since all interactions with the debugger are in PASCAL terms, users will not need to be familiar with the machine language of the host computer.
- Produces clear, complete error messages.
- Allows interprogram communication with other LPI languages.
- Provides a full set of listing options, including: annotated listing of the source program, user symbols, and their attributes; an annotated listing of the source cross-reference facility; and a summary of compilation statistics.

Items Included:

- PASCAL Compiler Software
- LPI-PASCAL Language Reference Manual
- LPI-PASCAL Quick Reference Guide
- LPI-PASCAL Release Notes
- LPI-PASCAL User's Guide

Requirements:

- 260 Kb RAM
- Software Generation Utilities (SLIN 0016GA)

BASIC Compiler

SLIN 0016EA

LPI-BASIC™ (from Language Processors, Inc.)

AT&T BASIC Interpreter

LPI-BASIC is an implementation of the ANSI-standard BASIC. It offers an extremely productive BASIC environment and allows easy conversion of existing application programs from Microsoft BASIC or CBASIC.

LPI-BASIC produces machine language that is extremely fast and efficient. This allows large, complex BASIC applications to be executed far faster than those developed with traditional BASIC interpreters.

Features:

- Can be debugged with LPI-DEBUG. Since all transactions with the debugger are in LPI-BASIC terms, users will not need to be familiar with the machine language of the host computer.
- Makes full use of LPI's global, local, and machine-dependent optimizations.
- Produces error messages in complete sentences, clearly identifying programming errors and often telling users how to correct them.
- Allows interprogram communication with subprograms written in any other LPI language.

BASIC Interpreter

AT&T's BASIC interpreter provides ANSI-BASIC capabilities. Programs developed with the BASIC interpreter provide immediate feedback. They can be compiled with the LPI-BASIC compiler to produce machine language that is extremely fast and efficient.

Items Included:

- BASIC Compiler
- Federal Systems Supplement to UNIX System V BASIC Language User's Guide
- LPI-BASIC Language Reference Manual
- LPI-BASIC Quick Reference Guide
- LPI-BASIC Release Notes
- LPI-BASIC User's Guide
- UNIX System V Basic Language User's Guide

Requirements:

- 200 Kb RAM
- Software Generation Utilities (SLIN 0016GA)

C Programming Language Utilities

SLIN 0016FA

AT&T C Language Compiler

The AT&T C Programming Language Utilities, Issue 4.2 is the standard C language compiler for AT&T computers.

Applications:

For applications of UNIX System V that require optical floating-point performance (engineering, science, mathematics, etc.).

Features:

- Assembly language programs not required
- Proprietary optimizer for floating-point operations
- Shared Library

Items Included:

- C Compiler Software
- Advanced C Utilities
- Extended Software Generation Utilities
- Source Code Control Utilities
- The C Programmer's Handbook
- AT&T UNIX System V Release 3.0, Programmer's Reference Manual
- AT&T 3B2 computer, UNIX System V, C Programming Language Utilities Issue 4.2 Release Notes
- AT&T 3B2 computer, UNIX System V, C Programming Language Utilities Issue 4.2 and Advanced Programming Utilities Issue 1.1 Product Overview
- Update for AT&T UNIX System V, Release 3.0 Programmer's Reference Manual

Requirements:

- 2.5 Mb disk space
- Software Generation Utilities (SLIN 0016GA)

Software Generation Utilities

SLIN 0016GA

AT&T Software Generation Utilities

AT&T's Software Generation Utilities provide development tools such as: assemble, link, and archive; object file utilities such as disassemble; strip, dump, nm and size utilities; and an object file optimizer.

AT&T's Software Generation Utilities incorporate libraries for software development: a C library (including a shared version), math library, debugging library, and profile library.

Applications:

Excellent source-level debugging where several languages are used.

Features:

- Provides effective tools used during software generations. These include assemble and link

Items Included:

- Software Generation Utilities
- AT&T UNIX System V Release 3.0 Programmer's Guide
- LPI CodeWatch Reference Manual
- LPI CodeWatch Release Notes

Requirements:

- One copy of the software is required for each 3B2/600G computer using one or more language processors.

MUMPS

SLIN 0016IA

MUMPS, an acronym for Massachusetts General Hospital Utility Multi-Programming System, is a high-level computer language with both programming and data base modes of operation.

MICRONETICS Standard MUMPS (MSM) is an entire data management system that does not require all the utilities, control blocks, and other "features" of COBOL-based systems. It is capable of handling large amounts of data in a simple, efficient manner. As a fourth generation language, MUMPS provides high programmer productivity and application flexibility.

Applications:

Applicable where multi-tasking, multi-user capabilities are required.

Features:

- Ease of programming
- ANSI Standard information processing
- Portability
- User-friendly

Items Included:

- MSM software for AT&T 3B2/600G computer
- MSM User's Guide
- MSM Language Reference
- MSM Utility Program Manual
- MSM Pocket Guide
- AT&T 3B2/600G Installation Guide

Requirements:

- 4 Mb memory
- 5 Mb available disk space

Electronic Filing

SLIN 0017AA

Prelude Central Filing Application

The Prelude central filing application stores and retrieves documents. A central directory is provided to store the most important documents; secondary directories are used for less significant files.

Features:

- Inserts, deletes, and moves files.
- Links files together before storing.
- Searches and retrieves files by name, key word, subject, or date.
- Allows users to view ASCII files on terminal, copy them to a UNIX system file, mail them to another user, or print them on a system printer.

Items Included:

- Electronic Filing Software
- Office Automation Guide

Requirements:

- Office Automation System (SLIN 0017RA)

Spreadsheet Utility

SLIN 0017BA

Prelude Spreadsheet

The Prelude spreadsheet is a screen-oriented application for financial planning. The spreadsheet performs a variety of calculations and can be used to build sophisticated models for budgeting, inventory control, and financial analysis.

A hierarchical menu structure makes the package extremely user-friendly.

Features:

- Inter-spreadsheet links to consolidate data
- Macros to automate routine tasks
- Windows for multiple displays
- Statistical tools for analyzing data
- 256 variable-size columns

Items Included:

- Spreadsheet Utility Software
- Spreadsheet and Graphics User's Guide

Requirements:

- Office Automation System (SLIN 0017RA)

Word Processor

SLIN 0017CA

Prelude Word Processor Interface

The Prelude word processor promotes productivity by providing screen-oriented text editing and formatting. Users can easily type documents, store and retrieve them, and merge text and graphics.

Automatic pagination and margin alignments allow users to review their documents before printing; they can see where the page ends, how a line breaks, or how a paragraph is formatted.

Windows allow users to switch back and forth between files to work on more than one project simultaneously. Forms can be stored and used as templates for applications such as invoicing and contracting.

The word processor can be used to convert files created with other word-processing packages for use in the Prelude environment — or to convert Prelude files for use with other word processing packages.

Features:

- Capability to merge text and graphics
- Forms storage
- Windowing

Items Included:

- Word Processor Software
- Word Processor User's Guide

Requirements:

- Office Automation System (SLIN 0017RA)

Spelling Corrector

SLIN 0017DA

Prelude Spelling Corrector

Prelude's interactive spelling corrector uses a primary, on-line dictionary of over 90,000 words. Users can create a personal secondary dictionary for words that are particular to their local environment or application.

Features:

- Automatic or selective search for incorrect words
- Lists of possible corrections
- Global or selective search and replacement
- Access from the text editor, word processor, or electronic mail programs

Items Included:

- Spelling Corrector Software
- Getting Started Guide

Requirements:

- Office Automation System (SLIN 0017RA)

Electronic Mail

SLIN 0017EA

Prelude Electronic Mail

Prelude mail allows users to send messages or files to a single user or groups of users. Each message identifies the date, time, sender, and subject.

The Prelude word processor can be used directly from the mail application to create and format messages. In addition, messages can be checked for spelling errors with the Prelude spell function.

Functions of Prelude mail include view, forward, print, file and delete.

Features:

- Word processor created messages
- Spell function can be used

Items Included:

- Electronic Mail Software
- Office Automation Guide

Requirements:

- Office Automation System (SLIN 0017RA)

Suspense/Task Management Utility

SLIN 0017FA

Prelude Task Manager

The Prelude task manager allows users to set up a "to do" list to track delegation and completion of tasks. This list is presented upon log-on or -off from system. Users can attach comments, a completion date, and a responsibility assignment
to a description of each task.

Tasks may be delegated through a hierarchical succession of users like links in a chain. Each "link" can attach comments, and the first link is notified when a task is completed.

Upon entering the task manager, a list of incomplete tasks is displayed on the screen, sorted by due date. Overdue tasks are marked with an asterisk and appear at the beginning of the list.

Menu options allow users to select more detailed information, including a report that will trace the delegation down the hierarchy of command.

Features:

- User-friendly menu
- Excellent tracking features

Items Included:

- Suspense/Task Management Utility
- Office Automation Guide

Requirements:

- Office Automation System (SLIN 0017RA)

Electronic Calendar Utility

SLIN 0017GA

Prelude Calendar

The Prelude calendar allows users to schedule personal appointments, group meetings, and office resources using a daily, weekly, or monthly calendar format.

Users can send notices of group meetings to each attendee by accessing the electronic mail function directly from their calendar. The calendar also includes tools for automatically archiving outdated appointments and for printing schedules. Users can even set alarms for crucial appointment times and send reminder notices of important appointments.

Items Included:
- Electronic Calendar Utility
- Office Automation Guide

Requirements:
- Office Automation System (SLIN 0017RA)

User Directory

SLIN 0017HA

Prelude User Information Application

The Prelude user information application allows users to determine the location of all users and groups of users on that system, providing the information needed for sending mail and scheduling meetings.

Each list is in tabular form, giving the user login name, as well as any other information the system administrator wishes to provide.

Features:
- Rapid access to information

Items Included:
- User Directory Software
- Office Automation Guide

Requirements:
- Office Automation System (SLIN 0017RA)

Electronic Authentication

SLIN 0017JA

Prelude Authentication Application

Prelude's authentication application allows users to place their own coded signature on a document and to validate the signatures of others. If a signature is invalid, a warning message will appear to show that the document was signed fraudulently.

Features:
- Menu-driven
- Easy to use

Items Included:
- Electronic Authentication Software
- Office Automation Guide

Requirements:
- Office Automation System (SLIN 0017RA)

Business Graphics Software

SLIN 0017KA

Prelude Business Graphics Package

The Prelude business graphics package can be used to generate six types of graphs:

- Bar charts
- Pie charts
- Line graphs
- Histographs
- Scattergrams
- Organization charts

This business graphics package accesses data from spreadsheets and data base tables. When necessary, it reformats the data to produce valid graphs.

Users can integrate graphs created with the business graphics package into reports or memos created with the word processor.

Applications:

Applicable when reports and memos are required to give easy-to-read information in spreadsheet or graphic format.

Features:
- Data from spreadsheets and data bases easily accessed
- Wide variety of chart formats

Items Included:
- Business Graphics Software
- Spreadsheet and Graphics User's Guide

Requirements:
- Office Automation System (SLIN 0017RA)

Statistical Analysis

SLIN 0017LA

Prelude Statistics Application

The Prelude statistics application offers tools for various kinds of analysis. Included are:

- Descriptive statistics to advanced regression
- Frequency charts
- Cross tabulations
- T-Tests

Features:

- Results can be edited, formatted, stored, or printed in a report
- Interactive calculator
- Text editor
- Six probability distribution functions
- Access to Prelude personnel data base and business graphics applications

Items Included:

- Statistical Analysis Software
- Spreadsheet and Graphics User's Guide

Requirements:

- 512 Kb RAM
- Office Automation System (SLIN 0017RA)

Project Management

SLIN 0017MA

Prelude Project Management Module

The Prelude project management module allows use of the "Critical Path Method" to track tasks according to time and resources. As tasks are added, changed, or deleted, the software recalculates and repaints the screen.

Features:

- Highlights critical tasks
- Provides five different screens for status tracking
  - Activity screen - uses GANTT chart to display standard end dates and to organize tasks
  - Network screen - shows relationship between various project activities
  - Calendar screen - provides a customized working schedule
  - Resource screen - shows personnel assignment along with periodic or fixed costs
  - Forecast screen - dual GANTT charts showing planned versus actual development of the project

Items Included:

- Project Management Software
- Project Manager User's Guide

Requirements:

- 512 Kb RAM
- Office Automation System (SLIN 0017RA)

Composition Graphics

SLIN 0017NA

AGILE Module

The AGILE composition graphics module is a complete line-art, graphics editor capable of single diagram and complex line drawings.

Applications:

For illustrating requirements involving line drawings.

Features:

- Flexibility in product design
- Library of more than 450 symbols
- Simplified editing operations
- Scaling
- Easily adjustable text attributes
- Four different user interfaces for different experience levels
- Exporting/importing text and graphics from various other applications
- Easy printing

Items Included:

- Composition Graphics Package
- AGILE Composition Graphics User's Guide

Requirements:

- Office Automation System (SLIN 0017RA)

Personal Filing

SLIN 0017PA

Provides facilities for establishing and managing personal files.

Items Included:

- Personal Filing Software
- Office Automation Guide

Requirements:

- Office Automation System (SLIN 0017RA)

Personal Database

SLIN 0017QA

Prelude Personal Database

The personal database is provided as an integral part of the basic office automation package. It provides facilities for managing mailing and phone lists.

Applications:

- Visual interface to a complete relational database
- Ability to merge with word processor mail

Items Included:

- Personal Database Software
- Office Automation Guide

Requirements:

- Office Automation System (SLIN 0017RA)

Office Automation System

SLIN 0017RA

Prelude Office Information System from VenturCom, Inc.

The integrated office automation system designed for SMSCRC includes a rich suite of integrated office automation applications. These range from word processing and spreadsheets to business graphics.

A data interchange capability allows users to share data, text, and graphics among components of the system. For example, spreadsheets created by the spreadsheet software package can be easily included in a document created by the word processor. U.S. Government-developed applications can be integrated into this flexible environment using Prelude interface tools.

The user interface for the Prelude Office Information System is consistent across all applications. It includes common menus, screen formats, keystrokes, and help messages.

Each element of the SMSCRC office automation system can be ordered individually (SLIN 0017AA through SLIN 0017QA).

Features:

- Electronic Filing
- Spreadsheet Utility
- Word Processor
- Spelling Corrector
- Electronic Mail
- Suspense/Task Management Facility
- Electronic Calendar
- Business Graphics
- Statistical Analysis Package
- Project Management
- Personal Filing
- Office Automation System
- User Directory
- Electronic Authentication
- Personal Database

Items Included:

- Office Automation Guide

Requirements:

- 512 Kb RAM
- 6 Mb disk space

Bar Code Software

SLIN 0018AA

AT&T Bar Code Utilities

AT&T Bar Code Utilities provide a robust interface between the AT&T 3B2/600G computer and bar code controller-decoders, hand-held terminals and line printers.

These utilities are accessible from the UNIX system shell. Single-character commands and user-friendly menus make the software easy to use.

Users can select the bar code operation required (receiving, transmitting, printing, or scanning) by stepping through various menus. Each menu guides through the steps necessary to complete the desired operation.

On-line, context-sensitive help is available at each step.

Features:

- User-friendly menus
- Single character commands

Items Supplied:

- Bar Code Software
- Bar Code Utilities UNIX Driver
- Bar Code Utility User's Guide

Requirements:

- Basic 3B2/600G computer with at least one EPORTS card
- Bar code equipment (SLINs 0011AA - 0011AE)

Trademarks

ACCELL, ACCELL/CP, RPT, and UNIFY are registered trademarks of Unify Corporation.
Ada is a registered trademark of the U.S. Government.
ASCENT is a trademark of Control Data Corporation.
CT-Mail is a trademark of Convergent Technologies, Inc.
dBase II and dBase III are registered trademarks and Framework is a trademark of Ashton-Tate, Inc.
DEC and DECdx are registered trademarks of Digital Equipment Corporation.
DisplayWrite 2, 3, and 4 are trademarks of International Business Machines Corporation.
Documenter's Workbench is a registered trademark of AT&T.
EtherLink is a trademark of 3Com Corporation.
EtherNet is a trademark of Xerox Corporation.
IBM is a registered trademark of International Business Machines.
KEYpak is a trademark of Keyword Office Technologies.
Lotus is a registered trademark of Lotus Development Corporation.
LPI, LPI-COBOL, LPI-BASIC, LPI-DEBUG, LPI-FORTRAN, and LPI-PASCAL are trademarks of Language Processors, Inc.
Level II COBOL is a trademark of Micro Focus, Inc.
MS-DOS, Multiplan, and Word are registered trademarks of Microsoft Corporation.
MultiMate is a registered trademark of Multimate International Corporation.
Multiplex is a trademark of Network Innovations Corporation.
Office Writer is a trademark of Office Solutions.
PC-Interface is a trademark of Locus Computing Corporation.
Prelude Office Information System is a trademark of VenturCom, Inc.
Q_ONE (UNIX) is a trademark of Quadratron Systems, Inc.
reQuest is a trademark of System Automation Corporation.
RM/COBOL is a trademark of Ryan-McFarland Corporation.
Samna and Word III are trademarks of Samna Corporation.
SQL is a tracemark of International Business Machines Corporation.
Symphony is trademark of Lotus Development Corporation.
TPlus is a trademark of Textware International.
TYMNET is a registered trademark of McDonnell Douglas.
UNIX is a registered trademark of AT&T.
VAX is a trademark of Digital Equipment Corporation.
OIS/VS, Wang PC, and Wang WITA are registered trademarks of Wang Laboratories.
WIN is a tracemark of the Wollongong Group, Inc.
WordMARC is a registered trademark of MARC Software International, Inc.
WordPerfect is a registered trademark of WordPerfect Corp.
WordStar is a registered trademark of MicroPro International Corp.
Xerox Writer II/III are registered trademarks of Xerox Corporation.

Every effort has been made to identify trademark information in the accompanying text. However, this information may have unintentionally been omitted in referencing particular products. Product names cited in the text, but not listed above, may also be trademarks of their respective manufacturers.

1.3 XTS-200/STOP

TARGET SYSTEM

DUAL PROCESSOR DPS 6 PLUS 8MBytes MIPS=1.7 GROWTH TO QUAD PROCESSOR 16 MBytes MIPS=3.2

Qty	MktID	Unit Purchase	Extended Purchase	GSA	MNTHLY MAINT	INITIAL SUPPORT	NOTE	Description
1	CPXA412-701	$57,000	$57,000	YES	$195	N/A	1	DPS600/412 DUAL CPU, 8MB, UPC/DSK'TE, (4) WS PORTS
1	CPF9960	$0	$0	YES	$0	N/A	1	(12) ADDITIONAL RS422 PORTS
1	PSS9906	$0	$0	YES	$0	N/A	1	1-PHASE 230 VOLT 60 CYCLE POWER
1	MSSA931-001	$21,000	$21,000	YES	$100	N/A	1	MXC-32F DISK CONTROLLER & (2) 295MB DISKS IN CABINET
1	MTM9905-001	$900	$900	YES	$9	N/A	1	UPC ADAPTER & 2 PORTS FOR 60/150MB QIC CRTRDGE TAPE
1	MTUA905-001	$1,780	$1,780	YES	$18	N/A	1	INTEGRATED 60MB QIC CARTRIDGE TAPE UNIT
5	HDS7506-001	$995	$4,975	YES	$8	N/A	1	BULL DISPLAY STATION MODEL 5, AMBER DISPLAY
5	CBL9915	$80	$400	YES	$0	N/A	1	25-FOOT RS422 CABLE FOR BDS-1,2,5, or 7
1	PRU7185	$1,195	$1,195	YES	$12	N/A	1	MODEL 21 MATRIX PRINTER, 136-COL 200/40-CPS RS422
1	I902802H	$17,268	$17,268	NO	N/A	N/A	3	TWO CHANNEL SECURE COMM SUBSYSTEM
1	I901602B	$7,500	$7,500	NO	TBD	$22,500	2	STOP 3.1 OPERATING SYSTEM LICENSE
1	I901401D	$1,300	$1,300	NO	TBD	$260	2	TCP/IP SOFTWARE LICENSE 1ST CONNECTION
1	I901401E	$1,000	$1,000	NO	TBD	$200	2	TCP/IP SOFTWARE LICENSE 2nd CONNECTION
		TOTAL	$114,318					

SOFTWARE DEVELOPMENT SYSTEM

DUAL PROCESSOR DPS 6 PLUS 8MBytes MIPS=1.7 GROWTH TO QUAD PROCESSOR 16 MBytes MIPS=3.2

Qty	MktID	Unit Purchase	Extended Purchase	GSA	MNTHLY MAINT	INITIAL SUPPORT	NOTE	Description
1	CPXA412-701	$57,000	$57,000	YES	$195	N/A	1	DPS600/412 DUAL CPU, 8MB, UPC/DSK'TE, (4) WS PORTS
1	CPF9960	$0	$0	YES	$0	N/A	1	(12) ADDITIONAL RS422 PORTS
1	PSS9906	$0	$0	YES	$0	N/A	1	1-PHASE 230 VOLT 60 CYCLE POWER
1	MSSA951-001	$32,000	$32,000	YES	$140	N/A	1	MXC-32F DISK CONTROLLER & (2) 595MB DISKS IN CABINET
1	MTM9905-001	$900	$900	YES	$9	N/A	1	UPC ADAPTER & 2 PORTS FOR 60/150MB QIC CRTRDGE TAPE
1	MTUA905-001	$1,780	$1,780	YES	$18	N/A	1	INTEGRATED 60MB QIC CARTRIDGE TAPE UNIT
6	HDS7506-001	$995	$5,970	YES	$8	N/A	1	BULL DISPLAY STATION MODEL 5, AMBER DISPLAY
6	CBL9915	$80	$480	YES	$0	N/A	1	25-FOOT RS422 CABLE FOR BDS-1,2,5, or 7
1	PRM9901	$550	$550	YES	$7	N/A	1	UPC ADAPTER FOR 325/650 LPM PRINTER
1	PRUA910-701	$8,700	$8,700	YES	$110	N/A	1	325 LPM 64 CHAR 136 COL LINE PRINTER
1	I902802H	$17,268	$17,268	NO	N/A	N/A	3	TWO CHANNEL SECURE COMM SUBSYSTEM
1	I901602B	$7,500	$7,500	NO	TBD	$22,500	2	STOP 3.1 OPERATING SYSTEM LICENSE
1	I901401D	$1,300	$1,300	NO	TBD	$260	2	TCP/IP SOFTWARE LICENSE 1ST CONNECTION
1	I901401E	$1,000	$1,000	NO	TBD	$200	2	TCP/IP SOFTWARE LICENSE 2nd CONNECTION
1	I901602C	1000	$1,000	NO	TBD	$3000	2	C COMPILER
1	I901602D	900	$900	NO	TBD	$2600	2	ADVANCED ASSEMBLER
1	I901602E	1500	$1,500	NO	TBD	$4500	2	SOFTWARE FACTORY
		TOTAL	$137,848					

Note 1 - One (1) year warranty/with all GSA prices subject to 10% discount
Note 2 - First year support fee paid in total amount with license fee and monthly beginning in 2nd year
Note 3 - Ninty (90) day warranty, maintenance on a time and material basis.

EXAMPLE CONFIGURATIONS and BUDGETARY PRICING AS OF APRIL 3, 1991

TARGET SYSTEM

DUAL PROCESSOR DPS 6000 16MBytes MIPS=5.7 GROWTH TO DUAL PROCESSOR 32 MBytes MIPS=5.7

Qty	MktID	Unit Purchase	Extended Purchase	GSA	MNTHLY MAINT	INITIAL SUPPORT	NOTE	Description
1	CPXA602-712	$91,000	$91,000	NO	$635	N/A	1	MODEL S62,16MB,290MBDISK,150MBTAPE,MLX16/(4)WS PORTS
1	CPFA960	$0	$0	YES	$0	N/A	1	(12) ADDITIONAL RS422 PORTS
1	MSUA953-082	$6,800	$6,800	NO	$40	N/A	1	SECOND 290MB DISK IN DPS6000 CABINET
6	HDS7506-001	$995	$5,970	YES	$8	N/A	1	BULL DISPLAY STATION MODEL 5, AMBER DISPLAY
6	CBL9915	$80	$480	YES	0	N/A	1	25-FOOT RS422 CABLE FOR BDS-1,2,5, or 7
1	PRU7185	$1,195	$1,195	YES	$12	N/A	1	MODEL 21 MATRIX PRINTER, 136-COL 200/40-CPS RS422
1	I902802H	$17,268	$17,268	NO	N/A	N/A	3	TWO CHANNEL SECURE COMM SUBSYSTEM
1	I901602B	$7,500	$7,500	NO	TBD	$22,500	2	STOP 3.1 OPERATING SYSTEM LICENSE
1	I901401D	$1,300	$1,300	NO	TBD	$260	2	TCP/IP SOFTWARE LICENSE 1ST CONNECTION
1	I901401E	$1,000	$1,000	NO	TBD	$200	2	TCP/IP SOFTWARE LICENSE 2nd CONNECTION
		TOTAL	$132,513					

SOFTWARE DEVELOPMENT SYSTEM

DUAL PROCESSOR DPS 6000 16MBytes MIPS=5.7 GROWTH TO DUAL PROCESSOR 32 MBytes MIPS=5.7

Qty	MktID	Unit Purchase	Extended Purchase	GSA	MNTHLY MAINT	INITIAL SUPPORT	NOTE	Description
1	CPXA602-712	$91,000	$91,000	NO	$635	N/A	1	MODEL S62,16MB,290MBDISK,150MBTAPE,MLX16/(4)WS PORTS
1	CPFA960	$0	$0	YES	$0	N/A	1	(12) ADDITIONAL RS422 PORTS
1	MSUA954-020	$15,200	$15,200	NO	$50	N/A	1	OUTBOARD DISK CABINET & (1) 590MB DISK
1	MSUA954-022	$13,200	$13,200	NO	$50	N/A	1	ADDITIONAL 590MB DISK
6	HDS7506-001	$995	$5,970	YES	$8	N/A	1	BULL DISPLAY STATION MODEL 5, AMBER DISPLAY
6	CBL9915	$80	$480	YES	0	N/A	1	25-FOOT RS422 CABLE FOR BDS-1,2,5, or 7
1	UPC9901	$2,000	$2,000	YES	$15	N/A	1	UNIVERSAL PERIPHERAL CONTROLLER (upc)
1	PRM9901	$550	$550	YES	$7	N/A	1	UPC ADAPTER FOR 325/650 LPM PRINTER
1	PRUA910-701	$8,700	$8,700	YES	$110	N/A	1	325 LPM 64 CHAR 136 COL LINE PRINTER
1	I902802H	$17,268	$17,268	NO	N/A	N/A	3	TWO CHANNEL SECURE COMM SUBSYSTEM
1	I901602B	$7,500	$7,500	NO	TBD	$22,500	2	STOP 3.1 OPERATING SYSTEM LICENSE
1	I901401D	$1,300	$1,300	NO	TBD	$260	2	TCP/IP SOFTWARE LICENSE 1ST CONNECTION
1	I901401E	$1,000	$1,000	NO	TBD	$200	2	TCP/IP SOFTWARE LICENSE 2nd CONNECTION
1	I901602C	1000	$1,000	NO	TBD	$3000	2	C COMPILER
1	I901602D	900	$900	NO	TBD	$2600	2	ADVANCED ASSEMBLER
1	I901602E	1500	$1,500	NO	TBD	$4500	2	SOFTWARE FACTORY
		TOTAL	$167,568					

Note 1 - One (1) year warranty/with all GSA prices subject to a 10% discount
Note 2 - First year support fee paid in total with license fee with monthly maintenance beginning 2nd year
Note 3 Ninty (90) day warranty, maintenance on a time and material basis.

EXAMPLE CONFIGURATIONS and BUDGETARY PRICING AS OF APRIL 3, 1991

TARGET SYSTEM
DUAL PROCESSOR DPS 6000 16MBytes MIPS=5.7 GROWTH TO QUAD PROCESSOR 64 MBytes MIPS=10.0

Qty	MktID	Unit Purchase	Extended Purchase	GSA	MNTHLY MAINT	INITIAL SUPPORT	NOTE	Description
1	CPXA621-701	$90,000	$90,000	YES	$300	N/A	1	DPS 6000/621,MONO,16MB,UPC/DSK'TE,MLX-16/(4)WS PORTS
1	CPFA960	$0	$0	YES	$0	N/A	1	(12) ADDITIONAL RS422 PORTS
1	CPKA601-701	$50,000	$50,000	YES	$300	N/A	1	MONO TO DUAL PROCESSOR UPGRADE
1	PSSA002-001	$0	$0	YES	$0	N/A	1	1-PHASE 230 VOLT 60 CYCLE POWER
1	MSSA931-001	$21,000	$21,000	YES	$100	N/A	1	MXC-32F DISK CONTROLLER & (2) 295MB DISKS IN CABINET
1	MTM9905-001	$900	$900	YES	$9	N/A	1	UPC ADAPTER & 2 PORTS FOR 60/150MB QIC CRTRDGE TAPE
1	MTUA931-002	$2,000	$2,000	YES	$20	N/A	1	INTEGRATED 150MB QIC CARTRIDGE TAPE UNIT
1	PRU7185	$1,195	$1,195	YES	$12	N/A	1	MODEL 21 MATRIX PRINTER, 136-COL 200/40-CPS RS422
5	HDS7506-001	$995	$4,975	YES	$8	N/A	1	BULL DISPLAY STATION MODEL 5, AMBER DISPLAY
5	CBL9915	$80	$400	YES	0	N/A	1	25-FOOT RS422 CABLE FOR BDS-1,2,5, or 7
1	I902802H	$17,268	$17,268	NO	N/A	N/A	3	TWO CHANNEL SECURE COMM SUBSYSTEM
1	I901602B	$7,500	$7,500	NO	TBD	$22,500	2	STOP 3.1 OPERATING SYSTEM LICENSE
1	I901401D	$1,300	$1,300	NO	TBD	$260		TCP/IP SOFTWARE LICENSE 1ST CONNECTION
1	I901401E	$1,000	$1,000	NO	TBD	$200		TCP/IP SOFTWARE LICENSE 2nd CONNECTION
		TOTAL	$197,538					

SOFTWARE DEVELOPMENT SYSTEM
DUAL PROCESSOR DPS 6000 16MBytes MIPS=5.7 GROWTH TO QUAD PROCESSOR 64 MBytes MIPS=10.0

Qty	MktID	Unit Purchase	Extended Purchase	GSA	MNTHLY MAINT	INITIAL SUPPORT	NOTE	Description
1	CPXA621-701	$90,000	$90,000	YES	$300	N/A	1	DPS 6000/621,MONO,16MB,UPC/DSK'TE,MLX-16/(4)WS PORTS
1	CPFA960	$0	$0	YES	$0	N/A	1	(12) ADDITIONAL RS422 PORTS
1	CPKA601-701	$50,000	$50,000	YES	$300	N/A	1	MONO TO DUAL PROCESSOR UPGRADE
1	PSSA002-001	$0	$0	YES	$0	N/A	1	1-PHASE 230 VOLT 60 CYCLE POWER
1	MSSA951-001	$32,000	$32,000	YES	$140	N/A	1	MXC-32F DISK CONTROLLER & (2) 595MB DISKS IN CABINET
1	MTM9905-001	$900	$900	YES	$9	N/A	1	UPC ADAPTER & 2 PORTS FOR 60/150MB QIC CRTRDGE TAPE
1	MTUA931-002	$2,000	$2,000	YES	$20	N/A	1	INTEGRATED 150MB QIC CARTRIDGE TAPE UNIT
1	PRM9901	$550	$550	YES	$7	N/A	1	UPC ADAPTER FOR 325/650 LPM PRINTER
1	PRUA910-701	$8,700	$8,700	YES	$110	N/A	1	325 LPM 64 CHAR 136 COL LINE PRINTER
5	HDS7506-001	$995	$4,975	YES	$8	N/A	1	BULL DISPLAY STATION MODEL 5, AMBER DISPLAY
5	CBL9915	$80	$400	YES	0	N/A	1	25-FOOT RS422 CABLE FOR BDS-1,2,5, or 7
1	I902802H	$17,268	$17,268	NO	N/A	N/A	3	TWO CHANNEL SECURE COMM SUBSYSTEM
1	I901602B	$7,500	$7,500	NO	TBD	$22,500	2	STOP 3.1 OPERATING SYSTEM LICENSE
1	I901401D	$1,300	$1,300	NO	TBD	$260	2	TCP/IP SOFTWARE LICENSE 1ST CONNECTION
1	I901401E	$1,000	$1,000	NO	TBD	$200	2	TCP/IP SOFTWARE LICENSE 2nd CONNECTION
1	I901602C	1000	$1,000	NO	TBD	$3000	2	C COMPILER
1	I901602D	900	$900	NO	TBD	$2600	2	ADVANCED ASSEMBLER
1	I901602E	1500	$1,500	NO	TBD	$4500	2	SOFTWARE FACTORY
		TOTAL	$219,993					

Note 1 - One (1) year warranty/with all GSA prices subject to 10% discount
Note 2 - First year support fee paid in total with license fee with monthly maintenance beginning 2nd year
Note 3 Ninty (90) day warranty, maintenance on a time and material basis.

EXAMPLE CONFIGURATIONS and BUDGETARY PRICING AS OF APRIL 3, 1991

SYSTEMS SOFTWARE

Qty	MktID	LICENSE FEE	SUPPORT FEE	GSA	Description
1	I9016028	$7,500	$22,500	NO	STOP 3.1
1	I901602C	$1,000	$3,000	NO	C LANGUAGE COMPILER
1	I901602D	$900	$2,600	NO	ADVANCED ASSEMBLER
1	I901602E	$1,500	$4,500	NO	SOFTWARE FACTORY
1	I901602F	$1,700	$5,300	NO	TRUSTED SWITCH
1	I901602G	$6,745	$2,500	NO	UNIPLEX-II PLUS 8 USER
1	I901401D	$1,300	$260	NO	TCP/IP/802.3 FIRST CONNECTION
1	I901401E	$1,000	$200	NO	TCP/IP/802.3 SECOND CONNECTION
1		$0	$0	NO	AT&T UNIX LICENSE

ALL SUPPORT FEES ARE ANNUAL PRICING WITH STOP 3.1 PAYABLE IN FULL FOR FIRST YEAR WITH LICENSE FEE

SYSTEMS DOCUMENTATION

MktID	UNIT PRICE	Description
71215482	N/C	XTS-200 STOP 3.1 SYSTEM RELEASE BULLETIN
71215483	$45	XTS-200 TRUSTED FACILITIES MANUAL
71215484	$60	XTS-200 USERS REFERENCE MANUAL
71215485	$30	XTS-200 ADMINISTRATORS GUIDE
71215799	$30	XTS-200 OPERATORS GUIDE
TBD	$150	XTS-200 BASE SET INCLUDES:71215483,71215484,71215485,71215799
TBD-1	$48	UNIPLEX II PLUS GUIDE
TBD-2	$27	UNIPLEX SYSTEM ADMINISTRATORS GUIDE
TBD-3	$9	UNIPLEX RELEASE/INSTALL NOTES
TBD-4	$7	UNIPLEX QUICK LOOK-UP GUIDE
TBD-5	$85	UNIPLEX BASE SET (TBD-1 THRU TBD-4
TBD-6	$37	UNIPLEX ADVANCED OFFICE SYSTEM USER GUIDE
TBD-7	$27	UNIPLEX CONFIGURATION GUIDE (6.01)
TBD-8	$40	TCP/IP USER'S GUIDE
TBD-9	$40	ISO USER'S GUIDE

BUDGETARY PRICING AS OF APRIL 3, 1991

COMMUNICATIONS SUBSYSTEM AND PROTOCOL SUPPORT

MKTG I.D.	DESCRIPTION	UNIT PRICE	ANNUAL MAINT
1) TCP/IP/802.3 CONNECTIONS			
A) ONE CHANNEL SCS			
I902801G	HARDWARE (1 CHANNEL)	$11,824	NOTE 3
I901401D	SOFTWARE LICENSE	$1,300	$260
B) TWO CHANNEL SCS			
I902802H	HARDWARE (2 CHANNEL)	$17,268	NOTE 3
I901401D	SOFTWARE LICENSE 1ST	$1,300	$260
I901401E	SOFTWARE LICENSE 2ND	$1,000	$200
C) FOUR CHANNEL SCS			
I902802J	HARDWARE (4 CHANNEL)	$32,848	NOTE 3
I901401D	SOFTWARE LICENSE 1ST	$1,300	$260
I901401E	SOFTWARE LICENSE 2ND/4TH	$3,000	$600
2) TP4/IP 802.3 CONNECTIONS			
A) ONE CHANNEL SCS			
I902801G	HARDWARE (1 CHANNEL)	$11,824	NOTE 3
	SOFTWARE LICENSE	$2,500	$500
B) TWO CHANNEL SCS			
I902802H	HARDWARE (2 CHANNEL)	$17,268	NOTE 3
	SOFTWARE LICENSE 1ST	$2,500	$500
	SOFTWARE LICENSE 2ND	$2,200	$440
C) FOUR CHANNEL SCS			
I902802J	HARDWARE (4 CHANNEL)	$32,848	NOTE 3
	SOFTWARE LICENSE 1ST	$2,500	$500
	SOFTWARE LICENSE 2ND/4TH	$6,600	$1,320
3) FDDI CONNECTIONS	(MKTG I.D. I910407)		
A) ONE CHANNEL SCS			
	HARDWARE (1 CHANNEL)	$38,446	NOTE 3
	SOFTWARE LICENSE 1ST	$1,300	$260
B) TWO CHANNEL SCS	HARDWARE (2 CHANNEL)	$51,752	NOTE 3
	SOFTWARE LICENSE 1ST	$1,300	$260
	SOFTWARE LICENSE 2ND	$1,000	$200
4) BASE SPS PRODUCT DEVELOPMENT (ONE TIME CHARGE)			
386 PC BASED SCS IMPLEMENTATION WITH TCP/IP FOR UNDERLYING SPS PROTOCOL IMPLEMENTATIONS		$13,132	N/A

BUDGETARY PRICING AS OF APRIL 3, 1991

COMMUNICATIONS SUBSYSTEM AND PROTOCOL SUPPORT

MKTG I.D.	DESCRIPTION	UNIT PRICE	ANNUAL MAINT
5) T1 CONNECTIONS	(PREREQ BASE SPS PRODUCT DEVELOPMENT)		
A) ONE CHANNEL SPS			
	HARDWARE (1 CHANNEL)	$38,464	NOTE 3
	SOFTWARE LICENSE 1ST	$1,300	$260
B) TWO CHANNEL SPS	HARDWARE (2 CHANNEL)	$44,908	NOTE 3
	SOFTWARE LICENSE 1ST	$1,300	$260
	SOFTWARE LICENSE 2ND	$1,000	$200
6) TCP/IP 802.5 TOKEN RING	(PREREQ BASE SPS PRODUCT DEVELOPMENT)		
A) ONE CHANNEL SPS			
	HARDWARE (1 CHANNEL)	$23,632	NOTE 3
	SOFTWARE LICENSE 1ST	$1,300	$260
B) TWO CHANNEL SPS			
	HARDWARE (2 CHANNEL)	$29,076	NOTE 3
	SOFTWARE LICENSE 1ST	$1,300	$260
	SOFTWARE LICENSE 2ND	$1,000	$200
7) TCP/IP/X.25 DDN	(PREREQ BASE SPS PRODUCT DEVELOPMENT)		
A) ONE CHANNEL SPS			
	HARDWARE (1 CHANNEL)	$22,756	NOTE 3
	SOFTWARE LICENSE 1ST	$1,300	$260
B) TWO CHANNEL SPS			
	HARDWARE (2 CHANNEL)	$28,200	NOTE 3
	SOFTWARE LICENSE 1ST	$1,300	$260
	SOFTWARE LICENSE 2ND	$1,000	$200
8) IP LABELING SUPPORT	(PREREQ BASE SPS PRODUCT DEVELOPMENT)		
	SOFTWARE	$1,376	N/A
9) MAXNET PORT TO STOP	(PREREQ BASE SPS PRODUCT DEVELOPMENT)		
	PORT COSTS	$16,512	N/A
10) DNSIX	(PREREQ BASE SPS PRODUCT DEVELOPMENT)		
	PORT COSTS	$4,128	N/A
11) DDCMP PROTOCOL INTERFACE	(PREREQ BASE SPS PRODUCT DEVELOPMENT)		
	SOFTWARE	$18,136	N/A
ONE TIME CHARGE FOR SPS PROTOCOL IMPLEMENTATIONS		$13,132	N/A

BUDGETARY PRICING AS OF APRIL 3, 1991

The above listed items are orderable under current Commercial Pricelists and will be provided in accordance with prices, terms and conditions in effect at the time the order is placed.

(1) THE INITIAL SUPPORT FEE, WHICH COVERS THE FIRST FULL YEAR OF SYSTEM SUPPORT, MUST BE ORDERED AT THE TIME OF THE LICENSE. ANNUAL AND/OR MONTHLY SUPPORT CHARGES COMMENCE WITH YEAR TWO (2).

1.4 GEMINI COMPUTERS

GEMINI TRUSTED MULTIPLE MICROCOMPUTER SYSTEM PRODUCTS

COMMERCIAL/OEM PRICE LIST

September 1987

BASE MODEL CONFIGURATIONS

The model numbers of Gemini products (e.g., W15-2 HP) identify the type of secondary storage, expansion capabilities, the number of processors, and processor performance. Gemini Multiprocessing Secure Operating System (GEMSOS) software is included with every model.

Three different types of secondary storage are offered. "R" models are RAM-based and require the purchase of optional non-volatile memory for loading GEMSOS and customer programs and data. They do not support self-hosting software development. "F" models provide one floppy diskette. "W" models provide one floppy and one 85 Mbyte Winchester hard disk. "W" models with the optional 140 Mbyte hard disk are recommended if software development is to be supported.

The first number following the storage identifier represents maximum expansion capability for processors. Models 6 and 9 can support only one processor. A Model 12 can support up to 2 processors. A Model 15 can support up to 3. A Model 26 can support up to 8 processors. After initial purchase, additional processors may be purchased as options and added to unused bus slots up to this expansion maximum for a given model.

The number following the hyphen indicates the number of processors in the base model.

Three processor performance classes are offered: Standard Performance, High Performance (HP) and Super Performance (SP). The standard and HP models use the 80286 CPU. SP models use the 80386 CPU. HP models have approximately twice the throughput of standard models. SP models have approximately three times the throughput of HP models.

All base models provide 512 Kb of global memory. The size of processor local memory varies with the type of processor. Standard and HP processors have 1 Mb of local RAM. SP processors have 2 Mb of local RAM. The sizes of global and local memory can be expanded. For self-hosting software development, one processor must have at least 2 Mb of local RAM on HP models or 4 Mb of local RAM on SP models.

Standard and HP models have two RS-232 serial I/O ports per processor. The Ethernet option (standard processor) replaces the serial ports. SP models have one serial port per processor.

GEMINI COMPUTERS, INC.

COMMERCIAL/OEM BASE MODEL PRICE LIST

September 1987

OEM prices are at a 1/3 discount from the prices shown on this page.

Gemini Trusted Computer Base	Model	Standard Performance Type	Standard Performance Price	High Performance Type	High Performance Price	Super Performance Type	Super Performance Price
RAM-based systems	R6 -1		26,835	HP	36,435	SP	55,335
	R12-1		33,023	HP	49,785	SP	80,835
	-2		61,793	HP	84,885	SP	131,985
	R15-1		36,210	HP	53,985	SP	89,835
	-2		64,980	HP	89,085	SP	140,985
	-3		84,165	HP	116,235	SP	180,735
Floppy diskette based system	F9 -1		43,313	HP	53,978	SP	83,228
	F12-1		46,500	HP	58,178	SP	89,228
One 5.25" HD diskette drive included.	-2		72,435	HP	95,528	SP	142,628
	F15-1		49,688	HP	62,378	SP	98,228
	-2		75,623	HP	99,728	SP	151,628
	-3		97,058	HP	129,128	SP	193,628
Winchester hard disk-based systems	W9 -1		53,813	HP	64,478	SP	93,728
	W12-1		57,000	HP	68,678	SP	99,728
	-2		82,935	HP	106,028	SP	153,128
One 85 Mb hard disk drive and one 5.25" HD diskette drive included.	W15-1		60,188	HP	72,878	SP	108,728
	-2		86,123	HP	110,228	SP	162,128
	-3		107,558	HP	139,628	SP	204,128
	W26-1		69,563	HP	85,262	SP	131,228
	-2		95,498	HP	122,612	SP	184,628
	-3		116,933	HP	152,012	SP	226,628
	-4		138,368	HP	181,412	SP	268,628
	-5		159,803	HP	210,812	SP	310,628
	-6		181,238	HP	240,212	SP	352,628
	-7		201,473	HP	268,412	SP	393,428
	-8		221,708	HP	296,612	SP	434,228

Gemini prices are subject to change without prior notice.

GEMINI COMPUTERS, INC.

COMMERCIAL/OEM HARDWARE OPTIONS PRICE LIST

September 1987

		COMMERCIAL PRICE	OEM PRICE
MEMORY			
o Additional Global or Local RAM:			
Volatile RAM	512 Kb	5,085	3,390
	1 Mb	8,456	5,637
	2 Mb	11,250	7,500
Non-volatile RAM	256 Kb	3,660	2,440
	512 Kb	6,120	4,080
	1 Mb	9,600	6,400
o Local RAM upgrade with system order:			
For Standard CPU			
1 Mb to 2 Mb		4,500	3,000
For HP CPU			
1 Mb to 2 Mb		4,500	3,000
1 Mb to 4 Mb		13,500	9,000
For SP CPU			
2 Mb to 4 Mb		9,000	6,000
2 Mb to 8 Mb		27,000	18,000
STORAGE			
o 360 Kb DS/DD Floppy Diskette		383	255
o 1.2 Mb HD Floppy Diskette		765	510
o 85 Mb Hard Disk		9,000	6,000
o 140 Mb Hard Disk		15,750	10,500
o 140 Mb Hard Disk upgrade ordered with "W" model		6,750	4,500
o Streaming Tape (120 Mb)		4,800	3,200
o 9 Track Magnetic Tape			
Tape Drive		24,750	16,500
Controller (for 1 or 2 drives)		9,750	6,500
INTERFACES			
o RS-232 serial I/O (8 Channels)		12,000	8,000
NETWORK INTERFACES			
o Ethernet (must be ordered with a standard CPU)		3,150	2,100
o X.25, HDLC LAPB controller		14,460	9,640

Gemini prices are subject to change without prior notice.

GEMINI COMPUTERS, INC.

COMMERCIAL/OEM SOFTWARE OPTIONS PRICE LIST

September 1987
Revised November 1987

	COMMERCIAL PRICE	OEM PRICE
SOFTWARE DEVELOPMENT ENVIRONMENT		
UNIX System V tools including an editor and one compiler, either Pascal or C		
o Self-hosted on Gemini computer		
. For HP models (requires 2 Mb RAM for one CPU)	10,125	6,750
. For SP models (requires 4 Mb RAM for one CPU)	22,500	15,000
o IBM PC-AT (requires 2 Mb RAM, 40 Mb hard disk, 1.2 Mb diskette, 8 Mhz or more)	2,625	1,750
Limit of 2 users per PC-AT	2,625	1,750
Unlimited users per PC-AT	2,999	1,999
o One additional compiler, Pascal or C		
. For standard or HP models or IBM PC-AT	1,043	695
. For SP models	1,425	950
o Sysgen Tools for F models (requires 1 Mb RAM for one CPU)	1,500	1,000
o Duplication and distribution of Kermit File Transfer Program	144	96
NON-KERNEL TCB SOFTWARE PACKAGE	5,550	3,700
Includes discretionary access controls, supporting policies, and support for distributed systems.		

Gemini prices are subject to change without prior notice.

CONFIGURATION OPTIONS

A wide range of options can be selected to augment any base model, within physical and logical limitations. The available items are shown on the Hardware and Software Options Price Lists. They can be added at the time of order, or, except where noted, at a later time with a moderate expansion cost in addition to the component cost.

VOLUME DISCOUNTS

The following volume discount schedule for Gemini computer systems and hardware components is offered for a single order of any mix of model types. Cumulative volume discounts will be negotiated on a case by case basis.

VOLUME DISCOUNT SCHEDULE FOR COMPUTER SYSTEMS

Number of units	5-9	10-24	25-99	100-249	Over 249
Discount	10%	20%	25%	30%	33%

The following software discount schedule applies to per-system fees for Gemini software products. These include GEMSOS for secure PC-AT workstations and the non-kernel TCB software package. Discounts do not apply to third-party development environment software.

SOFTWARE DISCOUNT SCHEDULE

QUANTITY	DISCOUNT
3-4	5%
5-6	10%
7-10	15%
11-15	20%
16-25	25%
26-40	30%
41-75	35%
76-140	40%
141-270	45%
271-550	50%
551-1,250	55%
1,251-3,300	60%
3,301-10,000	65%
10,001-25,000	70%
25,001-100,000	75%

UPGRADES

System upgrades after initial purchase are possible by either replacement or addition of components. They can usually be completed by the customer. Upgrades from a Model 9 to a Model 12 or 15, or from a Model 12 to a Model 15, are also possible. Quotations will be given on request.

DELIVERY

Both standard and HP Systems can be shipped 45 to 90 days after receipt of order depending on the configuration of the system ordered. Systems are shipped FOB Monterey, California. Invoices are submitted upon delivery net 30 days. Please contact Gemini for delivery commitment for SP Systems.

WARRANTY AND MAINTENANCE

Gemini systems are offered with a 90 day limited warranty against defects in material and workmanship. Factory maintenance can be purchased thereafter for a minimum period of one year payable quarterly in advance. GEMSOS software updates are free for one year after purchase. Continuing software updates and specified technical support are available for a minimum period of one year payable quarterly in advance. Quotations will be given on request.

TRAINING

Gemini offers software development training for GEMSOS programming to qualified engineers. Course information and prices are available on request.

2.0 SECURE COMMUNICATIONS

2.1 KG-84C General Purpose Encryption Equipment
2.2 AT&T STU-III Secure Data Device, Model 1900
2.3 GE STU-III/LCT 9600 Secure Communications Terminal

2.1 KG-84C General Purpose Encryption Equipment

KG-84C

General Purpose Encryption Equipment

FEATURES:

- Enables Transmissions of Secure Data via Standard Telegrapic Units
- Light Weight, Low Power Equipment
- Provides Encryption, Decryption of TTY and Data Traffic
- An MTBF of [illegible] Hours

Produced by: ALLIED [illegible]
Bendix [illegible]
1300 East Joppa [illegible]
Baltimore, M[illegible]

DESCRIPTION

The KG-84C General Purpose Telegraphy Encryption Equipment (GPTEE) is a lightweight, low power equipment for encryption/decryption of TTY and data traffic on dedicated links between various types of I/O devices and the KG-84C/KG-84A via a variety of modems. It enables the user to transmit secure data via standard telegraphic equipment over existing data lines.

OPERATION/ENVIRONMENTAL CAPABILITY

The KG-84C is designed to be man-transportable for use in tactical, mobile and protested locations, at all levels of command including vehicles, ships, aircraft and fixed plant environments. It has been fully qualified for severe environmental use.

The KG-84C can be easily rack mounted and has the same external housing and identical connectors as the KG-84A. However, it is not a direct replacement. For field use, an optional carrying case is available. It can be operated by local control at the front panel or remotely controlled. A wide variety of modems, and I/O equipment can be used directly or through a Data Adapter.

Additional capabilities include such new features as:

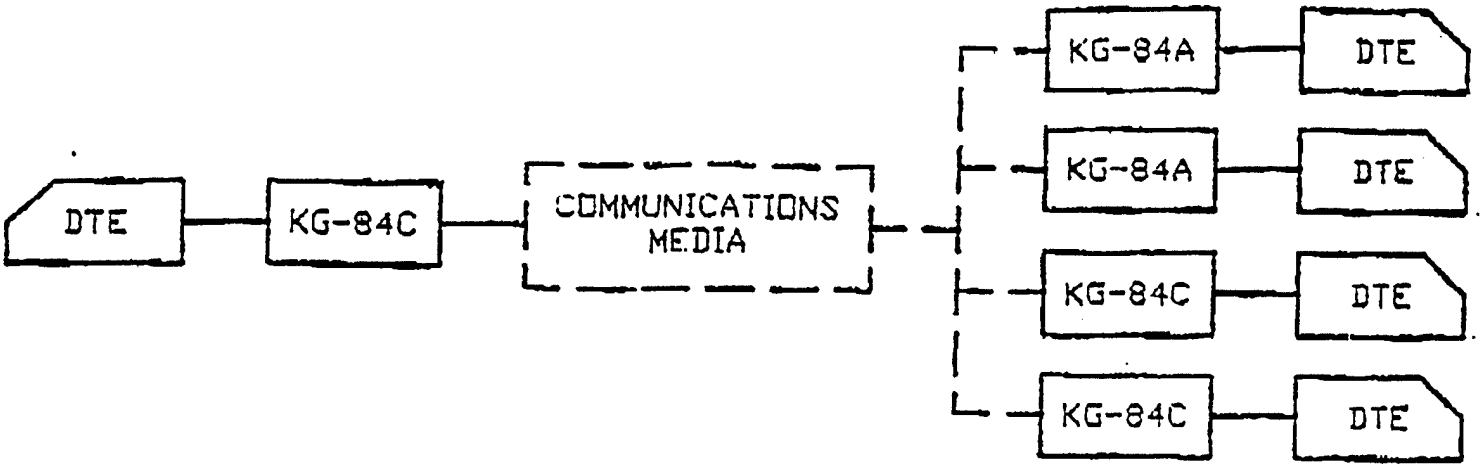
- Additional Synchronization Scheme for HF Radio.
- Asynchronous Black Side Output (CCITT R.101)
- Telex Compatibility (CCITT S.6 Automatic Plain Text Answer Back)
- Synchronous Out-of-Sync Detection
- Improved Self-Test Features
- Fewer internal Straps

TYPICAL OPERATING CONDITIONS

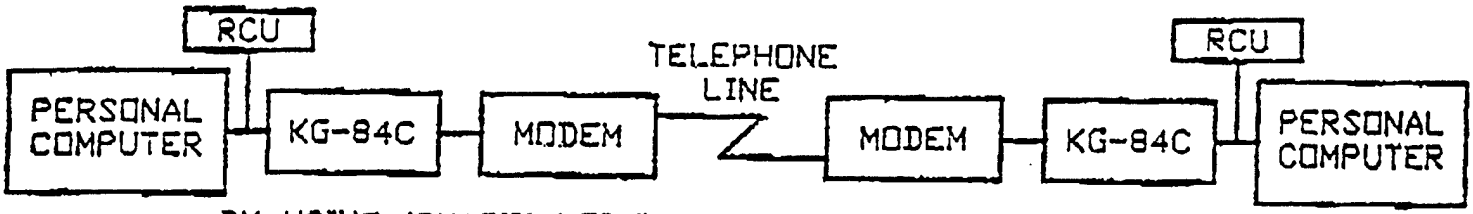
- High and Low Humidity
- Rain
- Vibration and Shock Environment
- Salt Fog
- Fungus
- Explosive Atmosphere
- Nuclear Survivability
- High and low Temperature - Altitude Combinations

SPECIFICATIONS

Size	19.1 CM (7.5 in) W, 37.46 CM (14.75 in) D. 19.98 CM (7.87 in) H
Operational Temperatures	-50° to 71°C
Power Options	19 to 30 Vdc. 24 Vdc Nominal
	115 Vac±15%, 45-66 Hz, Single Phase
20 W. Maximum Power Consumption	115 Vac±15%. 380 to 420 Hz, Single Phase
	230 Vac±15%. Unbalanced or Balanced 45 to 66 Hz (50 Hz Nominal), Single Phase
Unit Weight	10.2 Kg (22.5 Lbs)



INTEROPERABLE U.S. EQUIPMENT



BY USING 'SMART' MODEMS THE KG-84C WILL ALLOW PHONE DIALING FROM THE PERSONAL COMPUTER WHEN USING THE APPROPRIATE PC SOFTWARE AND THE REMOTE CONTROL OPTION.

PERSONAL COMPUTER COMMUNICATIONS

TELEX OPERATION

VARIOUS MODES OF OPERATION

CAPABILITY SUMMARY

- International Telegraph Alphabet Formats No. 2 and 5.
- Operating Rates 50 b/s to 32,000 b/s. With External Timing up to 64,000 b/s in Synchronous Data Mode.
- Full-Duplex or Simplex Mode Operation Either Point-to Point or Netted.
- AC or DC Primary Power Operation.
- Storage Battery for Retaining Keys
- Communications Options - Full-Duplex. Duplex independent, Transmit Only, Receive Only and Simplex.
- Clock Options

  Internal - Master Clock and Slave Clock Modes. Interfaces with Asynchronous Red and Black I/O Device.

  External - Data Rate Source, Station Clock and Red Side Terminal Source. Asynchronous Data Treated as Synchronous Data.

- Remote Control Options - from Either Black or Red Interface.
- Operating Controls and Indicators on Front Panel.

  - Mode Control Switch
  - Initiate/Indicator Test Switch
  - Enable/Zeroize Switch
  - Power Switch
  - Teletype Transmit Switch
  - Power On Indicator
  - Clear Text Indicator
  - Transmitter Ready Indicator
  - Receive Ready Indicator
  - Parity Indicator
  - Alarm Indicator
  - Variable Select Switch
  - Update Counter

- Concealed Controls on Front Panel.

  - Clock Select Switch
  - Data Rate Selector Switches
  - Step pulse Automatic with Data Length Setting
  - Teletype Mode Switch
  - Communication Mode Switch
  - Synchronization Mode Switch
  - Data Length Switch
  - Gated Clock Switch
  - Synchronous Out-of-Sync Selection Switch

APPLICABLE SPECIFICATIONS

- NSA SPEC 83-8
- EIA - RS-422A
  RS-423A
  RS-232C
  RS-449
- CCITT V.10
  V.11
  V.24
  R.101
  S.6
- MIL-STD-188-114

For additional information, please contact:

COMMUNICATION SYSTEMS TECHNOLOGY, INC.
Secure Telecommunications Division
9740 Patuxent Woods Drive
Columbia, Maryland 21046
(301) 381-5080

Communication Systems Technology, Inc.
Electronic Systems Development

Effective 01 September 1991

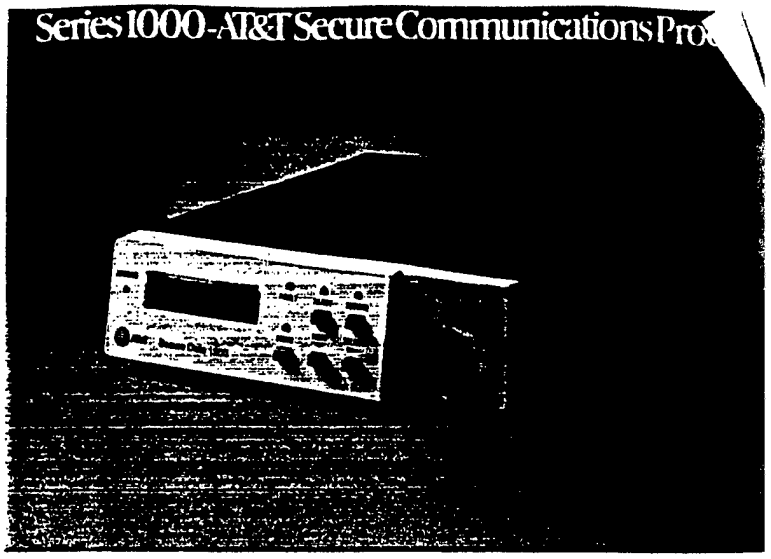
PRICE LIST

PART NO.	*DESCRIPTION*	*(1-50)*	*(51+)*
COMSEC			
KG-84A	COMSEC Device	$4,300	$3,900
KG-84C	COMSEC Device	$5,525	$5,300
KG-94/94A	COMSEC Device	$8,770	$8,390
KG-194/194A	COMSEC Device	$8,050	$7,730
KG-95	COMSEC Device	Inquire	Inquire
FILL DEVICES		*(1+)*	*(with KG)*
0N190315	KOI-18 Tape Reader	No longer available	
ON512424	Interface Cable	$225	$210
ACCESSORIES		*(1+)*	*(with KG)*
BA-1372/U	KG-84 Battery	$15	$15
ON231626	KG84 Power Cable	$245	$225
3031 S	Mosler Safe, with COMSEC Options, FPA/HNF, Power Supply, etc., to contain KG-84(),KG-94(),KG-194().	Inquire	Inquire
SERVICES	*(see Note 1)*	*(1)*	*(2+ same loc.)*
	Site Survey	$2,500	$1,500 each addl
	Installation	$3,500	$2,500 each addl
	(see Note 2)	*(1)*	*(2+ same loc.)*
	Site Survey	$3,000	$1,500 each addl
	Installation	$4,500	$2,500 each addl
		(1st hr.)	*(each addl hour)*
	Technical Support	$85*	

2.2 AT&T STU-III Secure Data Device, Model 1900

AT&T

AT&T STU-III Secure Data Device, Model 1900 For Secure, Classified Applications



The AT&T STU-III Secure Data Device, Model 1900, provides a simple and cost-effective way to protect *classified* government data transmissions. Developed under the U.S. Government's STU-III program, it's approved for use by federal departments, agencies and government contractors.

The Secure Data Device is part of an AT&T family of products for secure voice and data applications. Each is full-featured – and compact enough to be carried in your briefcase when you travel.

Doctrine governing these and other STU-III products is established and controlled by the government.

Protection for facsimiles, electronic mail and computer communications.

Whether you're accessing a computer data base, sending a fax or using electronic mail, you can be sure your information is protected – regardless of the classification level.

Cost-saving transmission over public and government switched networks.

The AT&T STU-III Secure Data Device can be used to transmit information over any public or government switched network at speeds of up to 9.6 kbps. You won't need an expensive, dedicated transmission path to assure data security.

Government approved for unattended operation.

The AT&T STU-III Secure Data Device is approved by the government for unattended secure data transmission.* As a result, facsimiles and other data communications can be sent to you even while you're away from your office.

Comprehensive service and support.

AT&T's toll-free hotline provides a single point of contact for comprehensive service and support. With a phone call you can resolve a question, place an order, troubleshoot problems, and more.

Repairs are hassle-free. If your terminal fails, we'll send you a replacement overnight. We're the *only* company in the industry to do so. And we stand behind the Secure Data Device with a full, two-year warranty with a one-year extension or five-year conversion.

Feature-rich.

AT&T designed the Secure Data Device with features and functions that lead the market and support our customers' special needs.

- **Access control.** The AT&T Secure Data Device is equipped with a unique Secure Access Control System (SACS) that brings unmatched flexibility to your data applications.

SACS allows you to establish a secure, closed network and to control access to facsimile machines or data stored on a PC or host computer. You simply program a list of authorized user IDs into your AT&T Secure Data Device. SACS automatically screens incoming calls, comparing the ID of the caller to those on your list. Unauthorized attempts are disconnected before the caller has access to your files.

Access can also be controlled by setting the device for minimum or maximum security levels. Only calls within the appropriate classification level will be accepted.

As an additional security feature, the AT&T Secure Data Device provides the information you need to maintain an audit trail of all attempts to access your network – whether successful or not.

- **Remote operation.** You can control the AT&T Secure Data Device remotely from any fax, PC or computer that is connected to its RS-232 data port. Remote commands are based on the Hayes® Smartmodem 2400™ command set.
- **Compatibility.** A full range of data speeds – from 2.4 kbps half duplex to 9.6 kbps full duplex – makes the AT&T device compatible with the secure data operation of any STU-III voice/data terminal.
- **Easy installation/operation.** The AT&T Secure Data Device is easy to install. You plug in the power cord and a telephone cord and connect the unit to your PC, facsimile machine or computer.

After completing an automated, key management procedure, the unit is ready to go secure. Rekeying is needed only once a year.

Operation is simple. No special training or cumbersome routines are required.

For more information.

The AT&T STU-III Secure Data Device can provide you with significant savings over traditional data security solutions. To find out more, call our toll-free number: **1-800-243-7883.**

*National and local security policies apply.

AT&T

AT&T STU-III Secure Data Device, Model 1900

Specifications

Information protected
- U.S. Government top secret, secret, confidential and unclassified

User community
- U.S. Federal Government
- U.S. Government contractors

Security features
- Secure Access Control System (SACS)
- Maximum and minimum security level setting
- Auto-answer, auto-secure
- Tempest
- CIK (crypto-ignition key)
- Active and passive
- terminal zeroization
- Fully automated STU-III fill procedures
- Display window for authentication identification
- Information to create a call audit trail

Key management
- Master CIK
- Traveling CIK
- Dual key sets
- Eight CIKs per key set

Secure data operational modes
- 9.6 kbps full-duplex sync/async
- 4.8 kbps full-duplex sync/async
- 2.4 kbps full-duplex sync/async
- 2.4 kbps half-duplex sync

Modem characteristics
- Near/far echo cancellation
- Frequency offset compensation
- 9.6 kbps: CCITT V.32 secure; sync/async; full duplex with optional trellis coding
- 4.8 kbps: CCITT V.32 secure; sync/async; full duplex
- 2.4 kbps: CCITT V.26 bis secure; sync/async; full duplex
- 2.4 kbps: CCITT v.26 bis secure; sync; half duplex
- Input level: 0 to -43 dBm
- Output level: adjustable, 0 to -15 dBm
- Automatic rate fallback: from 9.6 and 4.8 kbps to 2.4 kbps
- Remote control using Hayes AT commands

Interfaces
- External power supply
- EIA RS-232 data port with a 25-pin D-connector
- RJ11/RJ13 telephone jack to connect to public switched network, PABX or key systems
- RJ13 auxiliary set jack to connect standard telephone (optional)
- A/A1 leads (for use with key telephone systems)

Physical characteristics
- 8"w x 2.5"h x 9.5"d
- 7 lbs.
- Desktop or rack mountable

Environmental
- Operating temperature: 40° to 100°F
- Storage temperature: -40° to 150°F
- Relative humidity (storage): 5% to 95% noncondensing

Power
- External power supply selectable 90-134 VAC, 186-253 VAC
- Input frequency 47-63 Hz
- Input power dissipation 16 watts

Equipment interoperability (data mode)
- STU-III LCT, A and Cellular

Equipment compatibility
- Data devices with RS-232 output
- Digital facsimile

Compliance with standards
- FCC Part 15, Subpart J, Class B
- FCC Part 68
- UL 1459
- UL/TUV/CSA (power supply)
- Tempest NACSIM 5100A
- TSG5 — on-hook acoustic security
- MIL-STD-1472 Acoustical Noise, Curve NC-35
- EMC/EMI MIL-STD-461C
- ESD 20 kV
- 21 host-nation approvals

Warranty
- 24 months standard
- 12-month extension or 5-year conversion
- Post-warranty service available

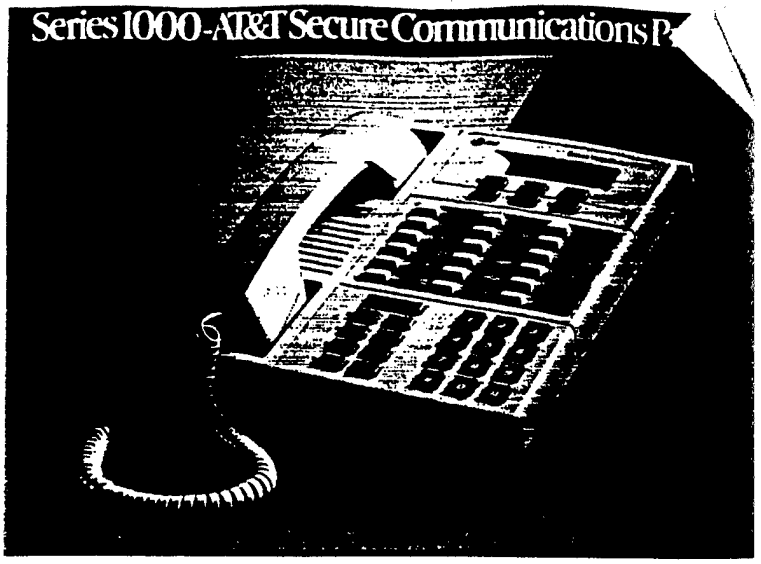
Options
- Carrying Case

Note:
Specifications subject to change without notice. U.S. Government regulations apply for purchase.

AT&T Federal Systems
Secure Communications Products
Customer Service Center, 71GC094041
P.O. Box 20046
Greensboro, NC 27420
Phone: **1-800-243-7883**

AT&T

AT&T STU-III Secure Voice/Data Terminal, Model 1100 For Secure, Classified Applications



The AT&T STU-III Secure Voice/Data Terminal, Model 1100, provides secure, classified voice and data communications in one integrated package.

It works both as a full-featured telephone for voice calls and as a smart modem for data applications. Part of an AT&T family of security products, the Voice/Data Terminal is compact and light enough to carry with you when you travel.

Developed under the U.S. Government's STU-III program, the terminal is approved for use by federal departments, agencies and government contractors.

Doctrine governing these and other STU-III products is established and controlled by the government.

One product for two jobs.

If you need both secure voice and secure data, the AT&T Secure Voice/Data Terminal can save you money. You won't need to clutter your desk with a secure phone *and* a secure modem.

Cost-saving transmission over public or government switched network.

AT&T's terminal is designed to secure both voice and data transmissions over public or government switched networks. You won't need an expensive, dedicated transmission path to assure security. Data can be transmitted at speeds of 2.4, 4.8 and 9.6 kbps — voice at 2.4 and 4.8 kbps.

Protection for facsimiles, electronic mail and computer communications.

Whether you're accessing a computer data base, sending a fax or using electronic mail, you can be sure your information is protected — regardless of the classification level.

Government approved for unattended operation.

The AT&T Secure Voice/Data Terminal is approved by the government for unattended secure data transmission.* As a result, facsimiles and other data communications can be sent to you even while you're away from your office.

Superior voice quality.

In the past, making a secure telephone call has meant compromising voice quality. That's not the case with the AT&T Secure Voice/Data Terminal. We've made certain that the voice quality of your secure calls will be comparable to that of your clear (non-secure) calls.

Comprehensive service and support.

AT&T's toll-free hotline provides a single point of contact for comprehensive service and support. With a phone call you can resolve a question, place an order, troubleshoot problems, and more.

Repairs are hassle-free. If your terminal fails, we'll send you a replacement overnight. We're the *only* company in the industry to do so. And we stand behind the Secure Voice/Data Terminal with a full, two-year warranty with a one-year extension or five-year conversion.

Feature-rich.

AT&T designed the Secure Voice/Data Terminal with features and functions that lead the market and support our customers' special needs.

- **Speakerphone.** A new built-in speakerphone gives you hands-free operation for secure and regular phone calls.
- **Access control.** The AT&T terminal is equipped with a unique Secure Access Control System (SACS) that brings unmatched flexibility to applications requiring security.

  SACS allows you to establish a secure, closed network for both voice and data communications. You can control access for secure phone calls or facsimile transmissions and protect data stored on a PC or host computer.

  To do so, you simply program a list of authorized user IDs into your AT&T terminal. SACS automatically screens incoming calls, comparing the ID of the caller to those on your list. Unauthorized attempts are disconnected before the caller has access.

  You can also control access by setting your terminal for minimum or maximum security levels. Only calls within the appropiate classification level will be accepted.

  As an additional security feature, the AT&T Secure Voice/Data Terminal provides the information you need to maintain an audit trail of all attempts to access your network — whether successful or disconnected.
- **Easy installation/operation.** Regardless of your application, the AT&T Secure Voice/Data Terminal is easy to set up and to operate. To install, you plug in the power cord and a telephone cord and connect the unit to your PC, facsimile machine or computer.

  After completing an automated, key management procedure, the unit is ready to go secure. Rekeying is needed only once a year.

  Operation is simple, and no special training is required.
- **Remote operation.** For data applications, you can control your AT&T Secure Voice/Data Terminal remotely from any fax, PC or computer connected to its RS-232 data port. Remote commands are based on the Hayes® Smartmodem 2400™ command set.
- **Compatibility.** The AT&T Secure Voice/Data Terminal is compatible with the more than 180,000 STU-III voice/data terminals currently fielded — and with the 1000 and 2000 Series of AT&T STU-III Secure Communications Products.

For more information.

The AT&T STU-III Secure Voice/Data Terminal provides a cost-effective approach to your security needs. To find out more, call our toll-free number: **1-800-243-7883.**

*National and local security policies apply.

AT&T

AT&T STU-III Secure Voice/Data Terminal, Model 1100

Specifications

Information protected
- U.S. Government top secret, secret, confidential and unclassified

User community
- U.S. Federal Government
- U.S. Government contractors

Security features
- Secure Access Control System (SACS)
- Fully automated STU-III fill procedures
- Maximum and minimum security level setting
- Display window for authentication identification
- Auto-answer, auto-secure
- Tempest
- Information to create a call audit trail
- CIK (crypto-ignition key)
- Active and passive terminal zeroization

Key management
- Master CIK
- Four key sets
- Traveling CIK
- Eight CIKs per key set

Voice modes
- Clear voice
- Secure voice
  - 4.8 kbps full-duplex CELP
  - 2.4 kbps full-duplex LPC10e
  - 4.8 kbps full-duplex HDLPC
  - 2.4 kbps half-duplex LPC10e

Telephone features
- Speakerphone — clear and secure
- Ringer volume control
- Ringer cutoff
- On hook dialing with speakerphone
- Handset volume control
- Microphone mute (disconnects microphone on both handset and speakerphone)
- Speakerphone volume control
- Pulse or tone dialing
- Last number redial
- 2-line by 16-character Liquid Crystal Display (LCD)
- Repertory dialing (32 numbers on single line; 20 numbers on multiline)
- PABX compatible
- Programmable pause
- Autovon precedence signaling clear and secure
- Dial tone detect
- Autovon preempt detection clear and secure
- Secure dialing
- Switch hook flash
- Multiline Model 1150 for use with 1A key systems (optional)
- Automatic disconnect
- Alerter volume control

Secure data operational modes
- 9.6 kbps full-duplex sync/async
- 2.4 kbps full-duplex sync/async
- 4.8 kbps full-duplex sync/async
- 2.4 kbps half-duplex sync

Modem characteristics
- Near/far echo cancellation
- 2.4 kbps: CCITT v.26 bis secure; sync; half duplex
- Frequency offset compensation
- 9.6 kbps: CCITT V.32 secure; sync/async; full duplex with optional trellis coding
- Input level: 0 to -43 dBm
- Output level: adjustable, 0 to -15 dBm
- 4.8 kbps: CCITT V.32 secure; sync/async; full duplex
- Automatic rate fallback: from 9.6 and 4.8 kbps to 2.4 kbps
- 2.4 kbps: CCITT V.26 bis secure; sync, async; full duplex

Interfaces
- External power supply, IEC 320/CEE-22 connector
- jack to connect to public switched network, PABX or key system
- EIA RS-232 data port with a 25-pin D-connector
- Autovon 2-wire
- RJ11/RJ13 telephone
- A/A1 leads (for use with key telephone systems)

Physical characteristics
- 9"w x 3.25"h x 11"d
- 10 lbs.

Environmental
- Operating temperature: +0° to 100°F
- Relative humidity (storage): 5% to 95% noncondensing
- Storage temperature: -40° to 150°F

Power
- External power supply selectable 90-134 VAC, 186-253 VAC
- Input frequency 47-63 Hz
- Input power dissipation 16 watts

Equipment interoperability
- STU-III LCT, A and Cellular

Equipment compatibility
- Data devices with RS-232 output
- Digital facsimile

Compliance with standards
- FCC Part 15, Subpart J, Class B
- MIL-STD-1472 Acoustical Noise, Curve NC-35
- FCC Part 68
- EMC, EMI MIL-STD-461C
- UL 1459
- ESD 20 kV
- UL TUV/CSA (power supply)
- HEMP-NSA 77-27
- Tempest NACSIM 5100A
- 21 host-nation approvals
- TSG 5 — on-hook acoustic security

Warranty
- 24 months standard
- Post-warranty service available
- 12-month extension or 5-year conversion

Options
- Carrying case
- Push-to-talk handset
- Multiline (5 lines and hold; to be used with 1A key systems)
- Uninterruptable power supply

Note:
Specifications subject to change without notice. U.S. Government regulations apply for purchase.

AT&T Federal Systems
Secure Communications Products
Customer Service Center, 71GC094041
P.O. Box 20046
Greensboro, NC 27420
Phone: **1-800-243-7883**

AT&T

AT&T Secure Communications Products Price Sheet

SERIES 1000: FOR CLASSIFIED GOVERNMENT APPLICATIONS

INTEGRATED VOICE AND DATA APPLICATIONS

	PRICE
• Model 1100 AT&T Secure Voice/Data Terminal (single line)	$2750
• Model 1100 quantity discount prices	
50-99	$2595
100-999	$2495
1000 or more	$2395
• Model 1150 AT&T Secure Voice/Data Terminal (multiline)	$3000
• Model 1150 quantity discount prices	
50-99	$2845
100-999	$2745
1000 or more	$2645
• Optional warranty extensions/conversions	
12-month warranty extension	$ 105
5-year warranty conversion	$ 315

DATA APPLICATIONS

	PRICE
• Model 1900 AT&T Secure Data Device	$2145
• Model 1900 quantity discount prices	
50-99	$2095
100-999	$2045
1000 or more	$1995
• Optional warranty extensions/conversions	
12-month warranty extension	$ 100
5-year warranty conversion	$ 300

Standard terms and conditions apply. Net 30 - FOB origin.
For more information, call 1-800-243-7883.

3/91

2.3 GE STU-III/LCT 9600 Secure Communications Terminal

GE STU-III 9600

GE STU-III 9600 . . . for dependable, secure communications.

The GE STU-III secure telecommunications instrument provides the most advanced secure voice and data capabilities available. Designed to contain all of the features of a modern office telephone, it also features secure voice and data transmission at the push of a button. In addition, over 25 years of experience at developing communications security (COMSEC) equipment for the U.S. Government goes into the making of the GE STU-III 9600 terminal. Along with this heritage comes the continued excellence in product warranty and support that GE is famous for throughout the industry and the world.

- **Full featured office telephone**
- **User friendly — simple to operate**
- **Compact size**
- **Superior voice quality — 4800 b/s CELP**
- **Versatile data communications for Fax, PC, Video, etc.**
  - **— 11 data rates include 9600/4800/2400 baud**
  - **— Remote access with access control - (SACS)**
  - **— Closed network capability**
  - **— A Hayes® like remote data protocol**
- **Built-in high reliability**

STU-III 9600

9600 Features *(STANDARD UNLESS INDICATED)*

- Universal Configuration — one model worldwide
- NSA Standard 2400 & 4800 b/s secure voice
- A Hayes® like data protocol for both attended and unattended operation
- Secure Access Control System (SACS) Includes the Multiple Keyset Access Control List, and Minimum and Maximum Security selection
- Speakerphone with on-hook dialing
- Autodialer (40 number - 32 digits including PAUSE, HOOKFLASH, PRECEDENCE, & P->T)
- Extended Reliability — MTBF: >20 years at normal usage rates
- Low Life Cycle Cost
- Supports 3 independent keysets, each with up to 8 Crypto Ignition Keys (CIKs)
- Interoperable Crypto Ignition Keys (up to 7 terminals)
- Password protection of all security features
- Autosecure on receive
- Nonsecure speech disable
- Built-in HEMP protection
- 40 Character SUPERTWIST LCD display (2 x 20)
- 2-wire AUTOVON capability
- Second network port — optional interfaces include: 4-wire AUTOVON; 2nd 2-wire; ISDN.
- Software settable modem level — eliminates RJ45
- Large data rate selection — 11 modes selectable
- Manual and automatic built-in-test (BIT)
- Universal Autoranging Power Supply — one model, worldwide
- Total Zeroization — with or WITHOUT POWER
- Tone (DTMF) and Pulse (rotary) dialing
- Full or Half duplex communication at all data rates
- HOOKFLASH button performs hook switch function for PABX/key systems features
- REDIAL — recalls last number dialed
- MUTE — disconnects microphones (handset & speakerphone)
- Anti-tamper design
- Software controlled/user prompts
- 4-wire AUTOVON capability — optional module on second port
- Multiline Accessory — optional custom modular extender
- Uninterruptible Power Supply (UPS) — optional
- Push-to-talk handset — optional

9600 Specifications

Telephone Set Configuration:	Standard single line (500/2500 type) and 1A2 multiline accessory available (5 line)
Voice Processors:	Government Standard Linear Predictive Coder (LPC-10) Enhanced @ 2400 b/s: Government Standard Codebook Excited Linear Predictive (CELP) @ 4800 b/s: Normal clear voice
Modems (internal):	Full or half duplex 2400 b/s V.26 ter, near and far end auto-ranging echo cancellation Full or half duplex 4800 b/s and 9600 b/s V.32, with frequency offset compensation
Telephone port:	Modular telephone jack RJ11C or RJ12C with A/A1 leads
Data Port:	9600, 4800 & 2400 b/s synch; 9600 to 75 b/s asynch RS232 compatible
COMSEC Subsystem:	All cryptologic functions (incl. SACS) contained in a protected subsystem

Power:	91 to 252 VAC, 47 to 63 Hz (autoselective); 2 Watts in standby; 20 Watts active
Operating Environment:	Temperature: 32° - 100° F (0° - 40°C) Relative Humidity—up to 90% non-condensing
MTBF:	>18,000 hrs. @ 100% duty cycle or >20 years @ normal usage rates
MTTR:	<1 hour
Industry Standards:	NSA approved FCC certified, Parts 15 & 68 EIA RS464, Bell PUB 48002 UL listed HEMP protection Tempest certified CONNECTION APPROVAL—granted or pending in all NATO nations and Australia, New Zealand, France, Sweden, & Switzerland

Logistics Support *1-800-521-9689*

- 15 Month warranty
- Extended Warranties/Service Contracts/Fixed Fee Repair
- Nationwide maintenance and user support provided by GE Computer Service
- Support systems to minimize user downtime
  - Functional modular design
  - Automated diagnostics (internal)
  - Loop tests (local/remote)
  - Repair and reship policy
  - Board level maintenance at local GE field offices (incl. Hawaii)

GE Aerospace
Government Communications Systems Department
Front & Cooper Sts./Bldg. 2-4

Camden, NJ 08102
Telephone 1-800 ALL STU 3
1-800- 255-7883
FAX (609) 338-2741

GE STU-III/LCT

SECURE COMMUNICATIONS TERMINALS
DIRECT SALES PRICE LIST
(Effective February 11, 1991)

		Part Number	Price
TERMINALS			
GE STU-III/LCT 9600	single line	10037828-501	$2540
	multiline	10037828-502	2610
GE STU-III/LCT 2400	single line*	8386621-501	2195
	multiline*	8386621-502	2325
ACCESSORIES			
Multiline Adapter for the GE STU-III/LCT 9600		10038073-501	149
Multiline Adapter for the GE STU-III/LCT 2400		8689417-501	149
Combination Second Telephone Line/Autovon Adapter for Model 9600		10038066-501	**
Universal Power Supply for GE STU-III/LCT 9600		10038064-1	149
Universal Power Supply for GE STU-III/LCT 2400		8572354-2	70
Uninterruptible Power Supply for GE STU-III/LCT 9600		10038603-501	365
Uninterruptible Power Supply Battery Pack		10038601-1	TBA
Standard Handset with Coiled Cord for the GE STU-III/LCT 9600		8572075-2	35
Push-to-Talk Handset with Coiled Cord for the GE STU-III/LCT 9600		8166795-2	50
Standard Handset with Coiled Cord for the GE STU-III/LCT 2400		8572075-1	30
Push-to-Talk Handset with Coiled Cord for the GE STU-III/LCT 2400		8166795-1	42
Batteries for GE STU-III/LCT 9600 (6-pack)		10038599-2	40
Batteries for GE STU-III/LCT 2400 (6-pack)		8572318-1	40
DC/DC Adapter for GE STU-III/LCT 9600		10038065-1	115
Blank Crypto-Ignition Key (KSD-64)	Call Datakey (612-890-6850) or CTS (612-536-3624)		
SERVICES			
12 month warranty extension			120
48 month warranty extension (5 year conversion)			480
12 month service contract			150
Post Warranty Repair & Return Service (Please call 1-800-521-9689 for Return Authorization)			585

For additional information or to place an order:

Call General Electric's STU-III Hotline

1-800-255-STU3 (7883)
1-609-338-6277
1-609-338-2741 (Fax)

or write to

General Electric Company
Government Communications Systems Department
Front & Cooper Streets, Bldg. 2-4
Camden, NJ 08102

NOTES

1. Terminals subject to export control and COMSEC account verification.
2. Each STU-III Terminal includes a Universal Power Supply, Standard Handset with Coiled Cord, Blank Crypto-Ignition Key, and User's Manual. Each Multiline Terminal Package also includes a Multiline Adapter.
3. All prices FOB origin.
4. Prices subject to change without notice.
5. TBA = To be Announced.

* Subject to Availability

** Call for Pricing Information

GE STU-III/LCT

SECURE COMMUNICATIONS TERMINALS
DIRECT SALES PRICE LIST
(Effective February 11, 1991)

		Part Number	Price
TERMINALS			
GE STU-III/LCT 9600	single line	10037828-501	$2540
	multiline	10037828-502	2610
GE STU-III/LCT 2400	single line*	8386621-501	2195
	multiline*	8386621-502	2325
ACCESSORIES			
Multiline Adapter for the GE STU-III/LCT 9600		10038073-501	149
Multiline Adapter for the GE STU-III/LCT 2400		8689417-501	149
Combination Second Telephone Line/Autovon Adapter for Model 9600		10038066-501	**
Universal Power Supply for GE STU-III/LCT 9600		10038064-1	149
Universal Power Supply for GE STU-III/LCT 2400		8572354-2	70
Uninterruptible Power Supply for GE STU-III/LCT 9600		10038603-501	365
Uninterruptible Power Supply Battery Pack		10038601-1	TBA
Standard Handset with Coiled Cord for the GE STU-III/LCT 9600		8572075-2	35
Push-to-Talk Handset with Coiled Cord for the GE STU-III/LCT 9600		8166795-2	50
Standard Handset with Coiled Cord for the GE STU-III/LCT 2400		8572075-1	30
Push-to-Talk Handset with Coiled Cord for the GE STU-III/LCT 2400		8166795-1	42
Batteries for GE STU-III/LCT 9600 (6-pack)		10038599-2	40
Batteries for GE STU-III/LCT 2400 (6-pack)		8572318-1	40
DC/DC Adapter for GE STU-III/LCT 9600		10038065-1	115
Blank Crypto-Ignition Key (KSD-64)	Call Datakey (612-890-6850) or CTS (612-536-3624)		
SERVICES			
12 month warranty extension			120
48 month warranty extension (5 year conversion)			480
12 month service contract			150
Post Warranty Repair & Return Service (Please call 1-800-521-9689 for Return Authorization)			585

For additional information or to place an order:

Call General Electric's STU-III Hotline

1-800-255-STU3 (7883)
1-609-338-6277
1-609-338-2741 (Fax)

or write to

General Electric Company
Government Communications Systems Department
Front & Cooper Streets, Bldg. 2-4
Camden, NJ 08102

NOTES

1. Terminals subject to export control and COMSEC account verification.
2. Each STU-III Terminal includes a Universal Power Supply, Standard Handset with Coiled Cord, Blank Crypto-Ignition Key, and User's Manual. Each Multiline Terminal Package also includes a Multiline Adapter.
3. All prices FOB origin.
4. Prices subject to change without notice.
5. TBA = To be Announced.

* Subject to Availability

** Call for Pricing Information