DEPARTMENT OF THE NAVY
NAVAL INFORMATION SYSTEMS
MANAGEMENT CENTER

ASSESSED PRODUCTS LIST
DRAFT

MODULE 10

INFORMATION SYSTEMS SECURITY
(INFOSEC)
PROGRAM GUIDELINES

DRAFT

Distribution: Submit requests for placement on distribution (including supporting justification), or amendment to the existing distribution, to:

Commanding Officer
NISE East
4600 Marriott Drive
North Charleston, SC 29406-6504

Commercial (803) 745-4600
DSN 563-2030

Stocked: Additional copies of NAVSO P-5239-10 can be obtained from the Navy Aviation Supply Office (Code 03415), 5801 Tabor Avenue, Philadelphia PA 18120-5099, through normal supply channels in accordance with NPFC PUB 2002D, NAVSUP P-437 or NAVSUP P-485, using AUTODIN, DAMES, or MILSTRIP message format to DAAS, Dayton, OH.

Cite stock number 0515-LP-208-8247.

Local reproduction is authorized.

DRAFT

DEPARTMENT OF THE NAVY

NAVAL INFORMATION SYSTEMS MANAGEMENT CENTER
WASHINGTON, D.C. 20360-5000

NAVSO P-5239-10
30 SEPTEMBER 1995

FOREWORD

This publication, Navy Staff Office Publication (NAVSO Pub) 5239, "Information Systems Security (INFOSEC) Program Guidelines" is issued by the Naval Information Systems Management Center. This publication consists of a series of modules providing procedural, technical, administrative and/or supplemental guidance for all information systems, whether business or tactical, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data. Each module will focus on a distinct program element, and will establish a standard methodology for planning, implementing and executing the INFOSEC program within the Department of the Navy (DON).

This module, "Assessed Products List", provides the Information Systems Security Manager (ISSM)/Automated Data Processing Security Officer (ADPSO) and system design and devegwpment personnel with information about evaluated and assessed Automated Information Systems (AIS) products and services. This document brings together the computer security products and services evaluated by the National Computer Security Center (NCSC), as well as those assessed by the Department of the Air Force and DON security organizations.

This module does not endorse any company's product, nor does it constitute certification or accreditation for the product's use in classified or sensitive environments. It only provides capability information for the listed products. Contact with agencies or activities outside DON channels with respect to information contained in this document must be made through the Commanding Officer, Naval Command, Control and Ocean Surveillance Center, In-Service Engineering, Code 043, 4600 Marriott Drive, North Charleston, South Carolina 29406-6504.

/s/
J. G. HEKMAN
Rear Admiral, SC, USN

THIS PAGE INTENTIONALLY BLANK

CONTENTS

Topic Page

Chapter 1 GENERAL INFORMATION ..... 1 - 1

1.1 Introduction ..... 1 - 1

1.2 Purpose ..... 1 - 1

1.3 Applicability and Scope ..... 1 - 2

1.4 References ..... 1 - 2

1.5 Terms Explained ..... 1 - 3

1.6 Future Guidebook Content ..... 1 - 4

Chapter 2 EVALUATED AND ASSESSED PRODUCTS ..... 2 - 1

2.1 General ..... 2 - 1

2.2 How to Use the Chapter's Information ..... 2 - 1

2.3 NCSC Evaluated Trusted Computing Base Operating Systems ..... 2 - 1

2.4 Security Packages for MS-DOS Micros, Workstations, and Personal Computers 2-37

2.5 Assessed Overwrite Tools 2-50

2.6 Assessed Trusted Applications 2-59

2.7 Other Assessed Security Products 2-60

Chapter 3 ASSESSED PRODUCTS ..... 3 - 1

3.1 DOS SECURITY PRODUCTS ..... 3 - 3

DECLASFY ..... 3 - 4

DeClass PC and FileZero PC ..... 3 - 5

DR DOS 6.0 Microcomputer Operating System ..... 3 - 10

Isolation System Access Control 2200 (ISAC 2200) ..... 3 - 14

LOCKIT I Extended Edition ..... 3 - 15

LOCKIT PROFESSIONAL ..... 3 - 17

Mace Utilities Version 1990.1 (DESTROY FILE Program) ..... 3 - 19

MAILSAFE Public Key Encryption ..... 3 - 21

Menu Works Advanced and Menu Works Total Security ..... 3 - 22

Modified Hard Disk Control Cable ..... 3 - 24

NoFBoot and SumFBoot ..... 3 - 25

Norton Commander ..... 3 - 27

Norton Utilities WIPEFILE and WIPEDISK Programs Ver 4.01 ..... 3 - 29

Norton Utilities Advanced Edition Programs (WIPEFILE and WIPEDISK) Ver. 4.5 ..... 3 - 30

Norton Utilities Advanced Edition WIPEFILE and WIPEDISK Programs on Combat Personnel Control System (CPCS) Z-248 ..... 3 - 32

Norton Utilities Advanced Edition WIPEFILE and WIPEDISK Programs on COMPAQ 386/25 ..... 3 - 34

Norton Utilities Advanced Edition WIPEFILE and WIPEDISK Programs on Sperry 3070-02 ..... 3 - 35

Norton Utilities Advanced Edition WIPEFILE and WIPEDISK Programs on UNISYS Desktop III ..... 3 - 36

Norton Utilities Programs Ver. 5.0 ..... 3 - 37

Norton Utilities Version 5.0 (WIPEINFO Program) ..... 3 - 39

Norton Utilities WipeInfo and DECLASFY Ver. 5.0 and 6.0 ..... 3 - 41

Norton Utilities WipeInfo 7.0 ..... 3 - 45

Norton Utilities WipeInfo 8.0 ..... 3 - 46

NoZFBoot ..... 3 - 47

ODCSOPS Automation Security Format (FILLDISK) Z-184 ..... 3 - 48

ODCSOPS Automation Security Format (FILLDISK) Z-248 ..... 3 - 49

ODCSOPS Automation Security Format (FILLDISK) on UNISYS Desktop III ..... 3 - 50

Overwrite Program to Declassify Floppy or Hard Disks (KILLDISK) Version 3.0 and 4.0 ..... 3 - 51

Overwrite Program to Declassify Floppy or Hard Disks (KILLDISK) Version 5.0 ..... 3 - 53

Overwrite Program to Declassify Floppy or Hard Disks (KILLDISK) on Combat Personnel Control System Z-248 ..... 3 - 54

Overwrite Program to Declassify Floppy or Hard Disks (KILLDISK) on COMPAQ 386/25 ..... 3 - 55

Overwrite Program to Declassify Floppy or Hard Disks (KILLDISK) on Sperry ..... 3 - 56

Overwrite Program to Declassify Floppy or Hard Disks (KILLDISK) on UNISYS Desktop III ..... 3 - 57

PC/DACS ..... 3 - 59

PCSecure ..... 3 - 60

PC Tools Deluxe Version 6 (CLEAR FILE Option) ..... 3 - 62

PC Tools Version 7 (WIPE Program) ..... 3 - 64

PC Tools Deluxe ..... 3 - 67

Personal Computer Security System ..... 3 - 69

PRIAM Hard Disk Formatting Software Programs ..... 3 - 70

RAMPART-PC Menu System ..... 3 - 72

Secure Electronic Bulletin Board System (SEBBS) ..... 3 - 74

Secure Copy Version 1.0 ..... 3 - 78

SECUREPC ..... 3 - 79

SecurePC and SecurePC PLUS ..... 3 - 80

TriSpan Workstation Manager (Trispan) ..... 3 - 82

V-PHAGE ..... 3 - 83

Watchdog ..... 3 - 85

Watchdog Armor ..... 3 - 86

3.2 MACINTOSH SECURITY PRODUCTS ..... 3 - 88

MacTools Deluxe ..... 3 - 89

Norton Utilities WipeInfo (Macintosh System) ..... 3 - 92

Symantec Utilities for MacIntosh ..... 3 - 93

The Viper ..... 3 - 95

VIPER ..... 3 - 97

3.3 SYSTEMS SECURITY PRODUCTS ..... 3 - 100

PC-Disk (AT&T 3B2/600G) ..... 3 - 101

Sanitization Software for the AT&T 3B2/600G ..... 3 - 103

3.4 ANTI-VIRAL PRODUCTS ..... 3 - 106

Disinfectant ..... 3 - 107

F-PROT Professional Anti-Virus Software ..... 3 - 109

VirHUNT ..... 3 - 110

VIRUSCAN ..... 3 - 112

VSHIELD ..... 3 - 114

3.5 UNIX SECURITY PRODUCTS ..... 3 - 116

Scrub Pro (part of Unishred Pro) ..... 3 - 117

Chapter 4 POINTS OF CONTACT ..... 4 - 1

APPENDIX A TRUSTED COMPUTING BASE SKETCHES ..... A - 1

APPENDIX B NCSC EVALUATED PRODUCTS ..... B - 1

ACF2 Release 3.1.3 ..... B - 2

Amdahl Corporation's UTS/MLS 2.1.5+ ..... B - 4

AOS/VS II ..... B - 6

Boot Protection Subsystem version 1.91 ..... B - 8

Compartmented Mode Workstation Plus (CMW+) Version 1.0 ..... B - 10

COMPSEC-II USA American Version, release B3.1 ..... B - 13

ConvexOS/Secure ..... B - 16

CX/SX Version 6.1.1 ..... B - 18

CX/SX with LAN/SX ..... B - 20

Gemini Trusted Network Processor (GTNP) ..... B - 22

HP-UX BLS ..... B - 26

IBM MVS/ESA EPL ..... B - 28

INFORMIX-OnLine/Secure ..... B - 30

INFORMIX-OnLine/Secure Release 5.0 ..... B - 32

LOCKIT Professional 2.10 ..... B - 35

MLS LAN Secure Network Server System ..... B - 37

MLS LAN ..... B - 39

OpenVMS VAX ..... B - 42

OS 1100/2200 Release SB4R7 ..... B - 44

Oracle 7 ..... B - 47

RAC/M and RAC/M II ..... B - 49

Resource Access Control Facility (RACF) ..... B - 51

SEVMS VAX ..... B - 53

System V/MLS Release 1.2.0 ..... B - 56

System V Release 4.1/ES ..... B - 58

Tandem Guardian 90 with Safeguard ..... B - 61

Tigersafe ..... B - 63

TOP SECRET ..... B - 65

Trusted IRIX/B ..... B - 67

Trusted Oracle 7 ..... B - 70

Trusted OS/32 with OS/32 MTM ..... B - 72

Trusted Solaris ..... B - 74

Trusted UNICOS 8.0 ..... B - 77

Trusted XENIX Version 2.0 ..... B - 80

Trusted XENIX Version 3.0 ..... B - 82

Trusted XENIX Version 4.0 ..... B - 84

ULTRIX MLS+ ..... B - 86

VSLAN 5.0 ..... B - 88

VSLAN 5.1 / VSLANE 5.1 ..... B - 91

WATCHDOG ..... B - 94

XTS-200 STOP 3.1.E ..... B - 96

APPENDIX C OTHER SECURITY PRODUCTS ..... C - 1

Access Managed Environment ..... C - 2

Certus ..... C - 3

Computer Security Toolbox ..... C - 5

Security Guardian ..... C - 6

Security Guardian ..... C - 8

TOVEN Secure Notebook ..... C - 10

SVS/OS CAP 1.00 ..... C - 11

Chapter 1

GENERAL INFORMATION

1.1 **Introduction**. This guidebook provides the Automated Information System (AIS) designer, developer, implementer, manager, and user with information about evaluated and assessed Information Systems Security (IawOSEC) products and services. Specifically, this guidebook provides:

a. A listing of computer security products and services evaluated by the National Computer Security Center (NCSC), as well as those assessed by U.S. Department of the Navy (DON) and U.S. Air Force security organizations. There are also matrices identifying those products that satisfy certain Trusted Computing Base protection standards, cited in DoD 5200.28-STD, DoD Trusted Computer Security Evaluation Criteria, 26 December 1985.

b. For NCSC evaluated products, an alphabetically arranged matrix summary and product assessment summaries. The information was extracted from the NSA Information Systems Security Products and Services Catalogue, 1995 Editions. Note that NSA publishes its catalogue twice per year (January and July) with updating supplements published in April and October.

c. For Navy and Air Force assessed products, executive summaries (contained in this guidebook) also arranged alphabetically by product name.

1.2 **Purpose**. AISs handle, produce, and store increasingly large amounts of sensitive and classified defense data which, if disclosed to unauthorized personnel, can compromise security or individual privacy. Likewise, inadvertent or intentional acts can also disclose, modify, or destroy data, and can disrupt or deny service to authorized users. Products are available which, when properly used, can reduce or eliminate such occurrences. This guidebook provides all interested DON activities with information on those computer security products that have undergone a structured assessment and evaluation by respective Navy, Air Force, and NCSC INFOSEC activities.

1.3 **Applicability and Scope**.

a. All DON personnel involved with AISs processing classified or sensitive unclassified information must take prudent steps necessary to protect that information from unauthorized disclosure, modification, or its denial to authorized users.

b. Proponents of many commercial and Government-developed security products often assert compliance with DoD security policies and standards. Responsible Service and Agency security activities examine those products and claims to assess their functionality, integrity, and security-related behavior. They then publish product official findings for use by cognizant persons who are responsible for AIS security. Within the DON, this responsibility and cognizance applies to system designers, developers, implementers, managers, maintainers, and users.

c. This guidebook has been organized as follows.

(1) This first chapter provides general overview, scope, and applicability information.

(2) Chapter 2 has individual sections listing security products (e.g., full featured Trusted Computing Base operating systems used on mainframe computers). Each section also has additional information about the product's security features, the standards it meets, a rating metric, and other details needed to assess its applicability for use within the DON. [Summaries for NCSC evaluated products may be found in the NSA Information Systems Security Products and Services Catalogue, April 1995 Edition. Note that NSA publishes its catalogue in January and July with updating supplements issued in April and October.]

(3) Chapter 3 includes executive summaries for Navy and Air Force assessed products. These summaries provide amplifying information regarding each product, as well as cautions and precautions for its use, and special conditions associated with its assessment. Collectively, this information gives cognizant security officials, who potentially might use the product, a basis to judge its merit for their specific systems and operational mission environment.

(4) The final chapter provides points of contact for the products and evaluating organizations.

(5) Appendices give synopses about Trusted Computing Base operating systems, paraphrased from NCSC technical publications.

1.4 **References**. The following references apply to this guidebook:

a. DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria, 26 December 1985.

b. DoD 5200.28, Security Requirements for Automated Information Systems (AISs), 21 March 1988.

c. NCSC-TG-005 Version 1, Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, 31 July 1987.

d. CSC-STD-005-85, DoD Magnetic Remanence Security Guideline, 15 November 1985.

e. NSA Publication, Information Systems Security Products and Services Catalogue, April 1992 Edition.

f. OPNAVINST 5239.1A, Department of the Navy Automatic Data Processing Security Program, 1 April 1985.

g. SECNAVINST 5239.2, Department of the Navy Automated Information System (AIS) Security Program, 15 November 1989.

h. Air Force Assessed Products List, November 1991.

i. NISE EAST 5239.1-G, Automated Information Systems Remanence Security Guidebook, 19 September 1990.

j. NAVSO P-5239-26, DON Remanence Security Guidebook, September 1993.

1.5 **Terms Explained**. The following terms apply to this guidebook:

a. **Assessed Products List (APL)**. Published by a Service or Agency security organization (other than NCSC), the APL gives findings and compliance information about security products which may have useful features that can enhance a system's security posture.

b. **Assessment**. A detailed examination conducted by a Service or Agency security organization, other than NCSC. An assessment subjects a computer security product to careful analysis and subsequent test scenarios, including TEMPEST compliance for those products containing hardware or firmware components.

c. **Evaluated Products List (EPL)**. Published by NCSC as a part of its Information Systems Security Products and Services Catalogue, the EPL gives authoritative findings and compliance information about operating systems and security packages having Trusted Computing Base safeguard features.

d. **Evaluation**. A formal, structured process, conducted by the National Security Agency, to determine the protection capabilities for commercially available and supported systems that meet the computer security needs of Government departments and agencies. To keep pace with evolving technology, some evaluated products undergo follow-on evaluation through the Ratings Maintenance Program (RAMP).

e. **Magnetic Remanence**. The residual magnetism representing recorded data that remains on magnetic storage media after degaussing. In the context of the APL, remanence refers to products claimed to clear or purge magnetic storage media in accordance with the provisions of NAVSO P-5239-26,DoN Remanence Security Guidebook, September 1993 and CSC-STD-005-85, DoD Magnetic Remanence Security Guideline, 15 November 1985.

f. **TCSEC**. The official short title for DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria, also known as the "Orange Book."

g. **Trusted Computing Base (TCB)**. A Trusted Computing Base (TCB) is a collection of hardware, operating system software, and procedures that meet a set of evaluation standards for protecting sensitive or classified information handled by an AIS. The NCSC publishes these standards in DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria, known as the "Orange Book."

1.6 **Future Guidebook Content**. This initial guidebook edition focuses on one of the three principaw disciplines within the INFOSEC domain (i.e., Computer Security). Future editions will incorporate Emanations Security (TEMPEST) and Communications Security (COMSEC) information. In the interim, if you need information about TEMPEST compliant or COMSEC products, please contact Code 042, at NISE EAST 4600 MARRIOTT DRIVE, NORTH CHARLETSON SC, 29406-6504.

Chapter 2

EVALUATED AND ASSESSED PRODUCTS

2.1 **General**. This chapter contains information about NCSC evaluated and Navy and Air Force assessed computer security products. It highlights their important security safeguard features and describes the standards used to rate their effectiveness. The chapter also provides information you need to weigh as you consider the products' applicability to your AIS and its operational scenarios, whether it is currently operational, being designed, or in acquisition. [You should take a few moments to scan Appendix A. It gives key concepts, in "plain English" format -- information that can help put evaluated and assessed products into perspective.]

2.2 **How to Use the Chapter's Information**. In subsequent chapter sections, you will find information about security products:

- Grouped according to the principal application served,
- Important security protection features,
- Criteria used to evaluate or assess them, and
- Summary matrices showing the rating achieved and some detail about the security feature components which led to the rating.

Before you begin your research, you may find it helpful to list important security protection features your AIS needs to have -- a rank-order list is ideal. Then, locate the section which best describes your situation (e.g., mainframe computer, security overwrite tool). With your list at hand, review the products most appropriate for your AIS' mission, user community, data sensitivity, and other factors. Keep in mind that no one security approach is always "best," rather, adaptations will need to be made in each case.

> Note
>
> Within the summary matrices, products have been arranged alphabetically so that you can find more detailed information readily in either NCSC's Information Systems Security Products and Services Catalogue, 1995 Editions, or in this guidebook (for Navy or Air Force assessed products).

2.3 **NCSC Evaluated Trusted Computing Base Operating Systems**. In 1987, DoD (C3I) issued a policy memorandum directing the Services and Agencies to implement trusted system safeguards meeting, at a minimum, Controlled Access Protection, by 1992. While few "trustworthy" operating systems existed at that time, there are several which have been developed

since then. In turn, these operating systems have been evaluated by the National Computer Security Center (NCSC) and been placed on their Evaluated Products List (EPL). System program managers, systems engineers, and their security engineering staffs can use the EPL to determine whether a particular computer platform has an available operating system which meets Controlled Access Protection, or higher, criteria.

a. **Features.** Controlled Access Protection operating systems, or more commonly known as Class C2, or just C2, provide basic system-enforced safeguards. For multiuser systems (and many other DON AISs as well), Controlled Access Protection provides a proper balance among operational mission functional requirements, procedural-enforced countermeasures, and security protection safeguards. For other AISs, both DoD and DON security policies require comprehensive safeguard techniques and/or additional assurances beyond those offered by Class C2. For example, mandatory access controls needed for system-enforced protection against compromise hazards occur in the "B" and higher classes only.

b. **Criteria**. NCSC's publication DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria (TCSEC, or the "Orange Book"), contains the criteria used to evaluate candidate trusted operating systems and their security safeguard features. In turn, the criteria stem from four fundamental security principles. Briefly, those principles are:

■ **SECURITY POLICY** reflects statutory requirements for how sensitive or classified information must be protected according to law. For example, such information must be marked, via labels, to distinguish it from information that may be freely requested or given. It also specifies the two ways statutory protection must be done: 1) "need-to-know" restrictions, done via discretionary access controls, and 2) authorization (or clearance), done via mandatory access controls. Finally, in the more stringent classes, SECURITY POLICY requires explicit controls be placed on the person or device requesting access, via the subject and device labels.

■ **ACCOUNTABILITY** further extends statutory requirements to positively identify and verify who is requesting access to information. By recording such access, via the audit features, personal accountability for actions taken can be fixed. Other techniques assure the user that the information sought is authentic and not a "forgery," that is, Trusted Path features guard against a malicious act or actor attempting to dupe the user.

■ **ASSURANCE** helps affirm how well the protection strategy implements statutory security policy requirements. It covers design, fabrication, and testing. It also assures there are in-place procedures and methods to conduct essential life-cycle maintenance and management activities, including configuration management techniques.

■ **DOCUMENTATION** must be published so the users and responsible facility security officials understand what the protection strategy is and how to use and maintain it properly throughout the system's life-cycle. Other documentation shows which tests were (or can be) used to affirm that the "as built" system properly meets statutory requirements, while the

Design Documentation cites which specific mechanisms, features, or functions implement the system's security policy.

Figure 2.3-1, adapted from the TCSEC, illustrates the safeguard mechanisms needed to meet class protection requirements. You can use the figure to help determine which specific safeguard features your particular mission, operational environment, user community, data sensitivity, and so on will need to have to comply with security policy directives. For example, you may be more concerned with who accesses your system than what functions they subsequently perform. Thus, you might select Class C2 for its Identification and Authentication features. By a similar reasoning process, you might need to know what functions your users perform, with less concern about who they are, and would select Class B1 with its more powerful audit features. In any event, while the minimum acceptable Trusted Computing Base operating system for DON use is Controlled Access Protection, your situation may require additional safeguards found in the "B1" and higher classes. You need to analyze your specific situation and make your selection accordingly. (Note: Naval Research Laboratory Report 8897 gives an easy to use methodology to help determine which trusted system class is appropriate for commonly encountered operational situations.)

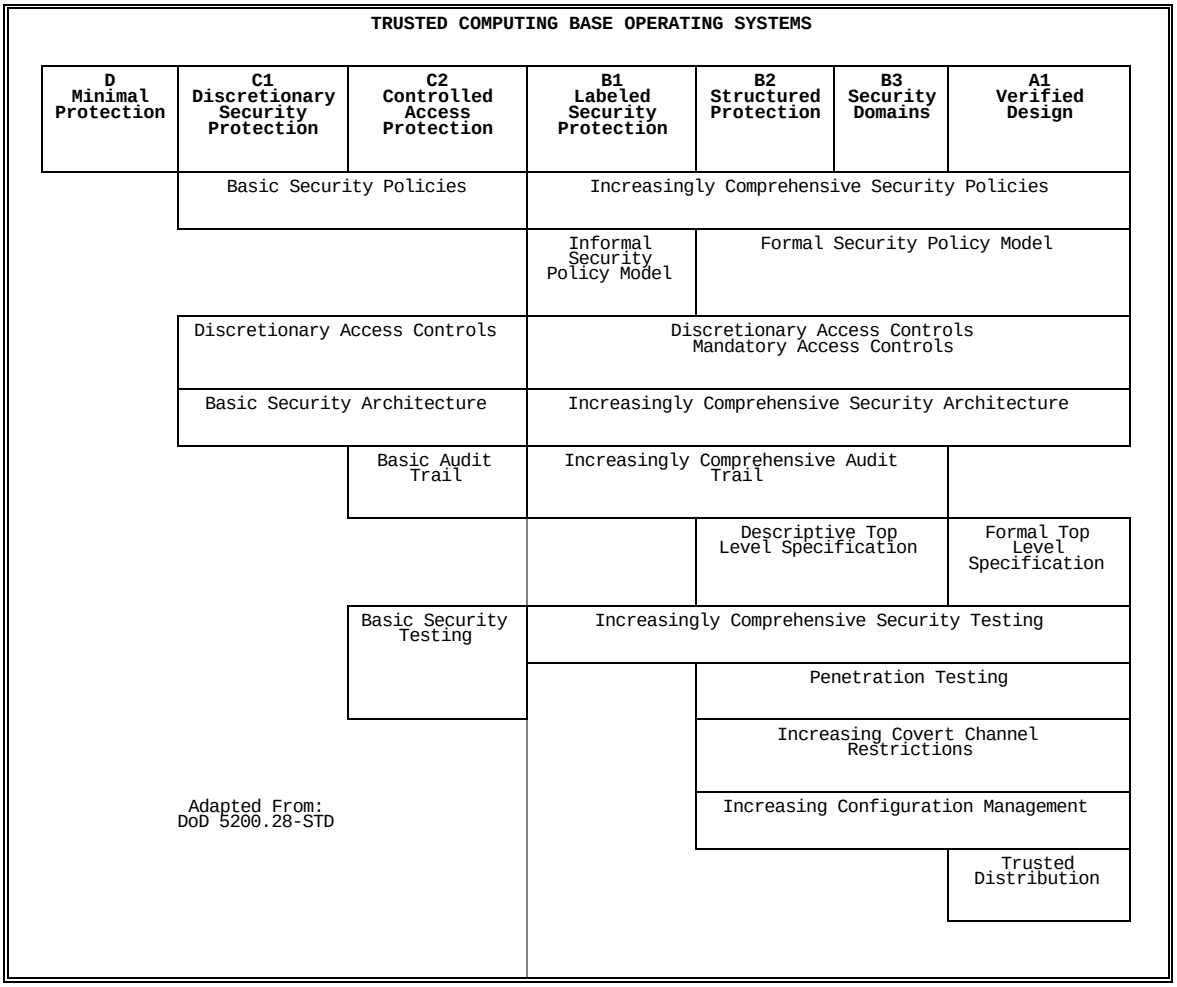

Figure 2.3-1

c. NCSC Evaluated Products Matrices. The matrices given below group NCSC evaluated operating systems and security safeguard packages according to the following scheme.

- Alphabetically, by product name.

- Platform, where platform may be: a Mainframe, Minicomputer, Workstation, Microcomputer, or Operating System.

You may want to scan Appendix A for information about the Rated Criteria shown in the matrices. For example, you will find "plain-English" explanations for Security Policy and its component elements explained there.

PRODUCT: IBM MVS/ESA Version 3 Release 3.1 — **OVERALL RATING** B1

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR **International Business Machines Corporation**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B3	System Architecture	B1	Security Feature User's Guide	B1
	Object Reuse	B1	System Integrity	B1	Trusted Facility Manual	B1
	Labels	B1	Security Testing	B1	Test Documentation	B1
	Label Integrity	B1	Design Specification and Verification	B1	Design Documentation	B1
	Exportation of Labeled Information	B1	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	B1	Trusted Facility Management	B2	**Accountability**	
	Exportation to Single-Level Devices	B1	Configuration Management	NR	Identification and Authentication	B1
	Labeling of Human-Readable Output	B1	Trusted Recovery	NR	Audit	B1
	Mandatory Access Control	B1	Trusted Distribution	NR	Trusted Path	NR
PLATFORMS **IBM 4381 Mid-Range to 3090 Mainframe Computers**	Subject Sensitivity Labels	NR				
	Device Labels	NR				

LEGEND: NA = Requirement is not applicable for this product NR = No requirements for this class
C = Meets CMW requirements W = Received CMW requirement waiver from DIA

PRODUCT: **Trusted XENIX Release 2.0**

OVERALL RATING B2

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR Trusted Information Systems, Inc. **PLATFORMS IBM PC AT, PS/2 Models 50, 60, 70, 70T, 70P and 80**[2]	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B3	System Architecture	B2	Security Feature User's Guide	B2
	Object Reuse	B2	System Integrity	B2	Trusted Facility Manual	B2
	Labels	B2	Security Testing	B2	Test Documentation	B2
	Label Integrity	B2	Design Specification and Verification	B2	Design Documentation	B2
	Exportation of Labeled Information	B2	Covert Channel Analysis	B2		
	Exportation to Multilevel Devices	B2	Trusted Facility Management	B3	**Accountability**	
	Exportation to Single-Level Devices	B2	Configuration Management	B2	Identification and Authentication	B2
	Labeling of Human-Readable Output	B2	Trusted Recovery	NR	Audit	B2
	Mandatory Access Control	B2	Trusted Distribution	NR	Trusted Path	B3
	Subject Sensitivity Labels	B2				
	Device Labels	B2				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: **Trusted XENIX Version 3.0** **OVERALL RATING B2**

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR Trusted Information Systems, Inc. PLATFORMS AST 386/25, GRID 1537, IBM PC AT, PS/2 Models 50, 60, 70, 70T, 70P and 80, NEC PowerMate 386/25, NEC Business Mate 386/25, Unisys Personal Workstation 2 Series 800 and Zenith Z-386/33	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B3	System Architecture	B2	Security Feature User's Guide	B2
	Object Reuse	B2	System Integrity	B2	Trusted Facility Manual	B2
	Labels	B2	Security Testing	B2	Test Documentation	B2
	Label Integrity	B2	Design Specification and Verification	B2	Design Documentation	B2
	Exportation of Labeled Information	B2	Covert Channel Analysis	B2		
	Exportation to Multilevel Devices	B2	Trusted Facility Management	B3	**Accountability**	
	Exportation to Single-Level Devices	B2	Configuration Management	B2	Identification and Authentication	B2
	Labeling of Human-Readable Output	B2	Trusted Recovery	NR	Audit	B2
	Mandatory Access Control	B2	Trusted Distribution	NR	Trusted Path	B3
	Subject Sensitivity Labels	B2				
	Device Labels	B2				

LEGEND: NA = Requirement is not applicable for this product NR = No requirements for this class
C = Meets CMW requirements W = Received CMW requirement waiver from DIA

PRODUCT: XTS-200
Version STOP 3.1.E

OVERALL RATING B3

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR HFS, Incorporated **PLATFORMS DPS 6 PLUS and DPS 6000**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B3	System Architecture	B3	Security Feature User's Guide	B3
	Object Reuse	B3	System Integrity	B3	Trusted Facility Manual	B3
	Labels	B3	Security Testing	B3	Test Documentation	B3
	Label Integrity	B3	Design Specification and Verification	B3	Design Documentation	B3
	Exportation of Labeled Information	B3	Covert Channel Analysis	B3		
	Exportation to Multilevel Devices	B3	Trusted Facility Management	B3	**Accountability**	
	Exportation to Single-Level Devices	B3	Configuration Management	B3	Identification and Authentication	B3
	Labeling of Human-Readable Output	B3	Trusted Recovery	B3	Audit	B3
	Mandatory Access Control	B3	Trusted Distribution	NR	Trusted Path	B3
	Subject Sensitivity Labels	B3				
	Device Labels	B3				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: Convex OS/Secure Version 10.0 **OVERALL RATING C2**

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR CONVEX Computer Corporation **PLATFORMS BSD 4.2 AND 4.3 UNIX**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B3	System Architecture	B1	Security Feature User's Guide	C2
	Object Reuse	C2	System Integrity	C2	Trusted Facility Manual	C2
	Labels	NR	Security Testing	C2	Test Documentation	C2
	Label Integrity	NR	Design Specification and Verification	NR	Design Documentation	C2
	Exportation of Labeled Information	NR	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	NR	Trusted Facility Management	B2	**Accountability**	
	Exportation to Single-Level Devices	NR	Configuration Management	NR	Identification and Authentication	C2
	Labeling of Human-Readable Output	NR	Trusted Recovery	NR	Audit	C2
	Mandatory Access Control	NR	Trusted Distribution	NR	Trusted Path	NR
	Subject Sensitivity Labels	NR				
	Device Labels	NR				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: **Trusted OS/32 with OS/32 MTM Release 08.03-3S**

OVERALL RATING C2

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR **Concurrent Computer Corporation**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	C2	System Architecture	B1	Security Feature User's Guide	C2
	Object Reuse	C2	System Integrity	C2	Trusted Facility Manual	C2
	Labels	NR	Security Testing	C2	Test Documentation	C2
	Label Integrity	NR	Design Specification and Verification	NR	Design Documentation	C2
	Exportation of Labeled Information	NR	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	NR	Trusted Facility Management	NR	**Accountability**	
	Exportation to Single-Level Devices	NR	Configuration Management	NR	Identification and Authentication	C2
	Labeling of Human-Readable Output	NR	Trusted Recovery	NR	Audit	C2
	Mandatory Access Control	NR	Trusted Distribution	NR	Trusted Path	NR
PLATFORMS **Concurrent 3280, 3280E and all members of Concurrent's Micro 3200 Family**	Subject Sensitivity Labels	NR				
	Device Labels	NR				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: **Tandem Guardian 90 with Safeguard Version S01.00**

OVERALL RATING C2

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR Tandem Computers Incorporated **PLATFORMS** **See Product Description**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B3	System Architecture	B1	Security Feature User's Guide	C2
	Object Reuse	C2	System Integrity	C2	Trusted Facility Manual	C2
	Labels	NR	Security Testing	C2	Test Documentation	C2
	Label Integrity	NR	Design Specification and Verification	NR	Design Documentation	C2
	Exportation of Labeled Information	NR	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	NR	Trusted Facility Management	NR	**Accountability**	
	Exportation to Single-Level Devices	NR	Configuration Management	NR	Identification and Authentication	C2
	Labeling of Human-Readable Output	NR	Trusted Recovery	NR	Audit	C2
	Mandatory Access Control	NR	Trusted Distribution	NR	Trusted Path	NR
	Subject Sensitivity Labels	NR				
	Device Labels	NR				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: SEVMS VAX Version 6.0 **OVERALL RATING B1**

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR Digital Equipment Corporation **PLATFORMS** **See Product Description**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B3	System Architecture	B1	Security Feature User's Guide	B1
	Object Reuse	B1	System Integrity	B1	Trusted Facility Manual	B1
	Labels	B1	Security Testing	B1	Test Documentation	B1
	Label Integrity	B1	Design Specification and Verification	B1	Design Documentation	B1
	Exportation of Labeled Information	B1	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	B1	Trusted Facility Management	NR	**Accountability**	
	Exportation to Single-Level Devices	B1	Configuration Management	NR	Identification and Authentication	B1
	Labeling of Human-Readable Output	B1	Trusted Recovery	NR	Audit	B1
	Mandatory Access Control	B2	Trusted Distribution	NR	Trusted Path	NR
	Subject Sensitivity Labels	NR				
	Device Labels	B2				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: **OpenVMS VAX Version 6.0 with VAXSMUP03_060**

OVERALL RATING C2

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR **Digital Equipment Corporation**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B3	System Architecture	B1	Security Feature User's Guide	C2
	Object Reuse	C2	System Integrity	C2	Trusted Facility Manual	C2
	Labels	NR	Security Testing	C2	Test Documentation	C2
	Label Integrity	NR	Design Specification and Verification	B1	Design Documentation	B1
	Exportation of Labeled Information	NR	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	NR	Trusted Facility Management	NR	**Accountability**	
	Exportation to Single-Level Devices	NR	Configuration Management	NR	Identification and Authentication	C2
	Labeling of Human-Readable Output	NR	Trusted Recovery	NR	Audit	C2
	Mandatory Access Control	NR	Trusted Distribution	NR	Trusted Path	NR
	Subject Sensitivity Labels	NR				
	Device Labels	NR				
PLATFORMS **Digital's Virtual Address Extension Processors**						

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: CX/SX Release 6.1.1 **OVERALL RATING B1**

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR Harris Computer Systems Division	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B1	System Architecture	B1	Security Feature User's Guide	B1
	Object Reuse	B1	System Integrity	B1	Trusted Facility Manual	B1
	Labels	B1	Security Testing	B1	Test Documentation	B1
	Label Integrity	B1	Design Specification and Verification	B1	Design Documentation	B1
	Exportation of Labeled Information	B1	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	B1	Trusted Facility Management	NR	**Accountability**	
PLATFORMS Series 4000 Night Hawk Product Line	Exportation to Single-Level Devices	B1	Configuration Management	NR	Identification and Authentication	B1
	Labeling of Human-Readable Output	B1	Trusted Recovery	NR	Audit	B1
	Mandatory Access Control	B1	Trusted Distribution	NR	Trusted Path	NR
	Subject Sensitivity Labels	B2				
	Device Labels	NR				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: HP-UX BLS Release 8.04 **OVERALL RATING B1**

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR Hewlett Packard Corporation	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B3	System Architecture	B1	Security Feature User's Guide	B1
	Object Reuse	B1	System Integrity	B1	Trusted Facility Manual	B1
	Labels	B1	Security Testing	B1	Test Documentation	B1
	Label Integrity	B1	Design Specification and Verification	B1	Design Documentation	B1
	Exportation of Labeled Information	B1	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	B1	Trusted Facility Management	B2	**Accountability**	
PLATFORMS HP9000/S800 Family of Computers	Exportation to Single-Level Devices	B1	Configuration Management	NR	Identification and Authentication	B1
	Labeling of Human-Readable Output	B1	Trusted Recovery	NR	Audit	B1
	Mandatory Access Control	B1	Trusted Distribution	NR	Trusted Path	NR
	Subject Sensitivity Labels	NR				
	Device Labels	NR				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: **Amdahl UTS/MLS Release 21.5+** **OVERALL RATING B1 (TCSEC)**

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR Amdahl Corporation	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B1	System Architecture	B1	Security Feature User's Guide	B1
	Object Reuse	B1	System Integrity	B1	Trusted Facility Manual	B1
	Labels	B1	Security Testing	B1	Test Documentation	B1
	Label Integrity	B1	Design Specification and Verification	B1	Design Documentation	B1
	Exportation of Labeled Information	B1	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	B1	Trusted Facility Management	NR	**Accountability**	
PLATFORMS Amdahl 5990 and 5995 Mainframes	Exportation to Single-Level Devices	B1	Configuration Management	NR	Identification and Authentication	B1
	Labeling of Human-Readable Output	B1	Trusted Recovery	NR	Audit	B1
	Mandatory Access Control	B1	Trusted Distribution	NR	Trusted Path	B2
	Subject Sensitivity Labels	B2				
	Device Labels	B2				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: AOS/VS II Release 3.01 **OVERALL RATING C2**

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR **General Data Corporation** **PLATFORMS** **Data General's ECLIPSE MV/Family Computers**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B3	System Architecture	B1	Security Feature User's Guide	C2
	Object Reuse	C2	System Integrity	C2	Trusted Facility Manual	C2
	Labels	NR	Security Testing	C2	Test Documentation	C2
	Label Integrity	NR	Design Specification and Verification	NR	Design Documentation	C2
	Exportation of Labeled Information	NR	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	NR	Trusted Facility Management	BR	**Accountability**	
	Exportation to Single-Level Devices	NR	Configuration Management	NR	Identification and Authentication	C2
	Labeling of Human-Readable Output	NR	Trusted Recovery	NR	Audit	C2
	Mandatory Access Control	NR	Trusted Distribution	NR	Trusted Path	NR
	Subject Sensitivity Labels	NR				
	Device Labels	NR				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: VSLAN 5.0

OVERALL RATING B2 MDIA Network Component

VENDOR
General Kinetics Corporation

PLATFORMS

See Product Description

RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
Security Policy		**Assurance**		**Documentation**	
Discretionary Access Control	B2	System Architecture	B2	Security Feature User's Guide	B2
Object Reuse	B2	System Integrity	B2	Trusted Facility Manual	B2
Labels	B2	Security Testing	B2	Test Documentation	B2
Label Integrity	B2	Design Specification and Verification	B2	Design Documentation	B2
Exportation of Labeled Information	B2	Covert Channel Analysis	B2		
Exportation to Multilevel Devices	B2	Trusted Facility Management	B2	**Accountability**	
Exportation to Single-Level Devices	B2	Configuration Management	B2	Identification and Authentication	B2
Labeling of Human-Readable Output	NA	Trusted Recovery	NR	Audit	B2
Mandatory Access Control	B2	Trusted Distribution	NR	Trusted Path	B2
Subject Sensitivity Labels	B2				
Device Labels	NA				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT:	**MLS LAN Secure Network Server System**		**OVERALL RATING A1 - MI Network Component**			
	RATING CRITERIA	**RATING**	**RATING CRITERIA**	**RATING**	**RATING CRITERIA**	**RATING**
VENDOR **Boeing Aerospace** **PLATFORMS** **See Product Description**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	NA	System Architecture	A1	Security Feature User's Guide	A1
	Object Reuse	A1	System Integrity	A1	Trusted Facility Manual	A1
	Labels	A1	Security Testing	A1	Test Documentation	A1
	Label Integrity	A1	Design Specification and Verification	A1	Design Documentation	A1
	Exportation of Labeled Information	A1	Covert Channel Analysis	A1		
	Exportation to Multilevel Devices	A1	Trusted Facility Management	NA	**Accountability**	
	Exportation to Single-Level Devices	A1	Configuration Management	A1	Identification and Authentication	A1
	Labeling of Human-Readable Output	NA	Trusted Recovery	A1	Audit	NA
	Mandatory Access Control	A1	Trusted Distribution	A1	Trusted Path	A1
	Subject Sensitivity Labels	A1				
	Device Labels	A1				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: **CS/SX with LAN/SX Release 6.1.1**

OVERALL RATING B1 MDIA Network Component

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR **Harris Computer Systems Division** **PLATFORMS** **Series 4000 Night Hawk Product Line**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B1	System Architecture	B1	Security Feature User's Guide	B1
	Object Reuse	B1	System Integrity	B1	Trusted Facility Manual	B1
	Labels	B1	Security Testing	B1	Test Documentation	B1
	Label Integrity	B1	Design Specification and Verification	B1	Design Documentation	B1
	Exportation of Labeled Information	B1	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	B1	Trusted Facility Management	NR	**Accountability**	
	Exportation to Single-Level Devices	B1	Configuration Management	NR	Identification and Authentication	B1
	Labeling of Human-Readable Output	B1	Trusted Recovery	NR	Audit	B1
	Mandatory Access Control	B1	Trusted Distribution	NR	Trusted Path	NR
	Subject Sensitivity Labels	B2				
	Device Labels	B1				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: Trusted UNICOS 8.0 Release 8.02

OVERALL RATING B1 MDIA

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR **Cray Research, Inc.** **PLATFORMS** **CRAY Y-MP Supercomputer Systems, including the C90, M90, E, and EL Series Supercomputers**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B3	System Architecture	B1	Security Feature User's Guide	B1
	Object Reuse	B1	System Integrity	B1	Trusted Facility Manual	B1
	Labels	B1	Security Testing	B1	Test Documentation	B1
	Label Integrity	B1	Design Specification and Verification	B1	Design Documentation	B1
	Exportation of Labeled Information	B1	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	B1	Trusted Facility Management	B2	**Accountability**	
	Exportation to Single-Level Devices	B1	Configuration Management	NR	Identification and Authentication	B1
	Labeling of Human-Readable Output	NA	Trusted Recovery	NR	Audit	B1
	Mandatory Access Control	B1	Trusted Distribution	A1	Trusted Path	NR
	Subject Sensitivity Labels	NR				
	Device Labels	NR				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: **MLS LAN Version 2.1**

OVERALL RATING A1 MDIA

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR **Boeing Aerospace**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	A1	System Architecture	A1	Security Feature User's Guide	A1
	Object Reuse	A1	System Integrity	A1	Trusted Facility Manual	A1
	Labels	A1	Security Testing	A1	Test Documentation	A1
	Label Integrity	A1	Design Specification and Verification	A1	Design Documentation	A1
	Exportation of Labeled Information	A1	Covert Channel Analysis	A1		
PLATFORMS	Exportation to Multilevel Devices	A1	Trusted Facility Management	A1	**Accountability**	
	Exportation to Single-Level Devices	A1	Configuration Management	A1	Identification and Authentication	A1
See Product Description	Labeling of Human-Readable Output	NA	Trusted Recovery	A1	Audit	A1
	Mandatory Access Control	A1	Trusted Distribution	A1	Trusted Path	A1
	Subject Sensitivity Labels	A1				
	Device Labels	A1				

LEGEND:NA = Requirement is not applicable for this productNR = No requirements for this class
C = Meets CMW requirementsW = Received CMW requirement waiver from DIA

PRODUCT: **Gemini Trusted Network Processor (GTNP) Version 1.01**

OVERALL RATING A1 Mandatory-Only Network Component

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR **Gemini Computers, Incorporated** **PLATFORMS** **Either an evaluated Gemini Trusted Base or an evaluated Gemini PC Workstation Lit for selected PC Compatibles**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	A1	System Architecture	A1	Security Feature User's Guide	A1
	Object Reuse	A1	System Integrity	A1	Trusted Facility Manual	A1
	Labels	A1	Security Testing	A1	Test Documentation	A1
	Label Integrity	A1	Design Specification and Verification	A1	Design Documentation	A1
	Exportation of Labeled Information	A1	Covert Channel Analysis	A1		
	Exportation to Multilevel Devices	A1	Trusted Facility Management	NA	**Accountability**	
	Exportation to Single-Level Devices	A1	Configuration Management	A1	Identification and Authentication	NA
	Labeling of Human-Readable Output	NA	Trusted Recovery	A1	Audit	NA
	Mandatory Access Control	A1	Trusted Distribution	A1	Trusted Path	NA
	Subject Sensitivity Labels	NA				
	Device Labels	A1				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: **INFOMIX-OnLine/Secure Release 4.1**

OVERALL RATING C2

VENDOR
Infomix Software, Inc.

PLATFORMS
AT&T System V/MLS 1.2.0 running System V3.1.1
Harris CX/SX Release 6.1.1
Harris CX/SX with LAN/SX Release 6.1.1
Hewlett Packard HP-UX BLS Release 8.04

RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
Security Policy		**Assurance**		**Documentation**	
Discretionary Access Control	C2	System Architecture	B1	Security Feature User's Guide	C2
Object Reuse	C2	System Integrity	C2	Trusted Facility Manual	C2
Labels	NR	Security Testing	C2	Test Documentation	C2
Label Integrity	NR	Design Specification and Verification	NR	Design Documentation	C2
Exportation of Labeled Information	NR	Covert Channel Analysis	NR		
Exportation to Multilevel Devices	NR	Trusted Facility Management	NR	**Accountability**	
Exportation to Single-Level Devices	NR	Configuration Management	NR	Identification and Authentication	B1
Labeling of Human-Readable Output	NR	Trusted Recovery	NR	Audit	B1
Mandatory Access Control	NR	Trusted Distribution	NR	Trusted Path	NR
Subject Sensitivity Labels	NR				
Device Labels	NR				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: **INFOMIX-OnLine/Secure Release 4.1**

OVERALL RATING B1

VENDOR
Infomix Software, Inc.

PLATFORMS
AT&T System V/MLS 1.2.0 running System V3.1.1
Harris CX/SX Release 6.1.1
Harris CX/SX with LAN/SX Release 6.1.1
Hewlett Packard HP-UX BLS Release 8

RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
Security Policy		**Assurance**		**Documentation**	
Discretionary Access Control	C2	System Architecture	B1	Security Feature User's Guide	C2
Object Reuse	C2	System Integrity	B1	Trusted Facility Manual	B1
Labels	B1	Security Testing	B1	Test Documentation	C2
Label Integrity	B1	Design Specification and Verification	B1	Design Documentation	B1
Exportation of Labeled Information	B1	Covert Channel Analysis	NR		
Exportation to Multilevel Devices	B1	Trusted Facility Management	NR	**Accountability**	
Exportation to Single-Level Devices	B1	Configuration Management	NR	Identification and Authentication	B1
Labeling of Human-Readable Output	B1	Trusted Recovery	NR	Audit	B1
Mandatory Access Control	B1	Trusted Distribution	NR	Trusted Path	NR
Subject Sensitivity Labels	NR				
Device Labels	NR				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: **Oracle7 Version 7.0.13**

OVERALL RATING C2

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR Oracle Corporation	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	C2	System Architecture	B1	Security Feature User's Guide	C2
	Object Reuse	C2	System Integrity	C2	Trusted Facility Manual	C2
	Labels	NR	Security Testing	B1	Test Documentation	C2
	Label Integrity	NR	Design Specification and Verification	NR	Design Documentation	C2
	Exportation of Labeled Information	NR	Covert Channel Analysis	NR		
PLATFORMS HP-UX BLS	Exportation to Multilevel Devices	NR	Trusted Facility Management	NR	**Accountability**	
	Exportation to Single-Level Devices	NR	Configuration Management	NR	Identification and Authentication	B1
	Labeling of Human-Readable Output	NR	Trusted Recovery	NR	Audit	B1
	Mandatory Access Control	NR	Trusted Distribution	NR	Trusted Path	NR
	Subject Sensitivity Labels	NR				
	Device Labels	NR				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: **Trusted Oracle7**
Version 7.0.13

OVERALL RATING B1

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR **Oracle Corporation** **PLATFORMS** **See Product Description**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	C2	System Architecture	B1	Security Feature User's Guide	C2
	Object Reuse	C2	System Integrity	B1	Trusted Facility Manual	B1
	Labels	B1	Security Testing	B1	Test Documentation	C2
	Label Integrity	B1	Design Specification and Verification	B1	Design Documentation	B1
	Exportation of Labeled Information	B1	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	B1	Trusted Facility Management	NR	**Accountability**	
	Exportation to Single-Level Devices	B1	Configuration Management	NR	Identification and Authentication	B1
	Labeling of Human-Readable Output	B1	Trusted Recovery	NR	Audit	B1
	Mandatory Access Control	B1	Trusted Distribution	NR	Trusted Path	NR
	Subject Sensitivity Labels	NR				
	Device Labels	NR				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: **CMW+ for A/UX Version 1.0**

OVERALL RATING B1

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR SecureWare, Inc. PLATFORMS Macintosh IIx and Macintosh IIcx[2]	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B3	System Architecture	B1	Security Feature User's Guide	B1
	Object Reuse	B1	System Integrity	B1	Trusted Facility Manual	B1
	Mandatory Access Control	W	Security Testing	B1	Test Documentation	B1
	Sensitivity Labels	B1	Design Specification and Verification	B1	Design Documentation	B1
	Sensitivity Label Integrity	B1	Trusted Facility Management	C		
	Exportation of SL Information	B1	Configuration Management	B2	**Accountability**	
	Exportation to Multilevel SL Devices	B1	Trusted Recovery	C	Identification and Authentication	B1
	Exportation to Single-Level SL Devices	B1	Trusted Distribution	A1	Audit	W
	Labeling of Human-Readable Output	NR			Trusted Path	B3
	Device Sensitivity Labels	B1				
	Window Sensitivity Labels	NR				
	Information Labels	C				
	Information Label Integrity	C				
	Window Information Labels	C				
	Input Information Labels	C				
	Exportation of IL Information	C				
	Exportation to Multilevel IL Devices	C				
	Exportation to Single-Level IL Devices	C				
	Changing Information Labels	C				
	Inter-Window Moves	C				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: System V/MLS Version 1.2.0u — **OVERALL RATING B1**

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR **American Telephone and Telegraph Co.** **PLATFORMS** **AT&T 3B2/500 and AT&T 3B2/600 Minicomputers**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B1	System Architecture	B1	Security Feature User's Guide	B1
	Object Reuse	B1	System Integrity	B1	Trusted Facility Manual	B1
	Labels	B1	Security Testing	B1	Test Documentation	B1
	Label Integrity	B1	Design Specification and Verification	B1	Design Documentation	B1
	Exportation of Labeled Information	B1	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	B1	Trusted Facility Management	NR	**Accountability**	
	Exportation to Single-Level Devices	B1	Configuration Management	NR	Identification and Authentication	B1
	Labeling of Human-Readable Output	B1	Trusted Recovery	NR	Audit	B1
	Mandatory Access Control	B2	Trusted Distribution	NR	Trusted Path	B2
	Subject Sensitivity Labels	B2				
	Device Labels					

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: SVS/OS CAP Version 1.01 **OVERALL RATING C2**

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR **Wang Laboratories, Inc.** **PLATFORMS** **Wang VS Product Family**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	C2	System Architecture	B1	Security Feature User's Guide	C2
	Object Reuse	C2	System Integrity	C2	Trusted Facility Manual	C2
	Labels	NR	Security Testing	C2	Test Documentation	C2
	Label Integrity	NR	Design Specification and Verification	NR	Design Documentation	C2
	Exportation of Labeled Information	NR	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	NR	Trusted Facility Management	NR	**Accountability**	
	Exportation to Single-Level Devices	NR	Configuration Management	NR	Identification and Authentication	C2
	Labeling of Human-Readable Output	NR	Trusted Recovery	NR	Audit	C2
	Mandatory Access Control	NR	Trusted Distribution	NR	Trusted Path	NR
	Subject Sensitivity Labels	NR				
	Device Labels	NR				

LEGEND: NA = Requirement is not applicable for this product NR = No requirements for this class
C = Meets CMW requirements W = Received CMW requirement waiver from DIA

PRODUCT: Trusted XENIX Version 4.0 **OVERALL RATING B2**

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR **Trusted Information Systems, Inc.** **PLATFORMS** **AST 386/25, GRID 1537, IBM PC AT, PS/2 Models 50, 60, 70, 70T, 70P and 80, NEC PowerMate 386/25, NEC Business Mate 386/25, UnisysPersonal Workstation 2 Series 800 and Zenith Z-386/33**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B3	System Architecture	B2	Security Feature User's Guide	B2
	Object Reuse	B2	System Integrity	B2	Trusted Facility Manual	B2
	Labels	B2	Security Testing	B2	Test Documentation	B2
	Label Integrity	B2	Design Specification and Verification	B2	Design Documentation	B2
	Exportation of Labeled Information	B2	Covert Channel Analysis	B2		
	Exportation to Multilevel Devices	B2	Trusted Facility Management	B3	**Accountability**	
	Exportation to Single-Level Devices	B2	Configuration Management	B2	Identification and Authentication	B2
	Labeling of Human-Readable Output	B2	Trusted Recovery	NR	Audit	B2
	Mandatory Access Control	B2	Trusted Distribution	NR	Trusted Path	B3
	Subject Sensitivity Labels	B2				
	Device Labels	B2				

LEGEND: NA = Requirement is not applicable for this product NR = No requirements for this class
C = Meets CMW requirements W = Received CMW requirement waiver from DIA

PRODUCT: VSLANE Version 5.1 — **OVERALL RATING B2 MDIA**

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR **General Kinetics Corporation (Formerly Verdix)** **PLATFORMS** **See Product Description**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B2	System Architecture	B2	Security Feature User's Guide	B2
	Object Reuse	B2	System Integrity	B2	Trusted Facility Manual	B2
	Labels	B2	Security Testing	B2	Test Documentation	B2
	Label Integrity	B2	Design Specification and Verification	B2	Design Documentation	B2
	Exportation of Labeled Information	B2	Covert Channel Analysis	B2		
	Exportation to Multilevel Devices	B2	Trusted Facility Management	B2	**Accountability**	
	Exportation to Single-Level Devices	B2	Configuration Management	B2	Identification and Authentication	B2
	Labeling of Human-Readable Output	B2	Trusted Recovery	NR	Audit	B2
	Mandatory Access Control	B2	Trusted Distribution	NR	Trusted Path	B2
	Subject Sensitivity Labels	B2				
	Device Labels	B2				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: OS 1100/2200 Release SB4R7 — **OVERALL RATING B1**

	RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
VENDOR **UNISYS Corporation** **PLATFORMS** **UNISYS 1100/90, 2200/100, 2200/200, 2200/400, 2200/600, 2200/600ES & 2200/900**	**Security Policy**		**Assurance**		**Documentation**	
	Discretionary Access Control	B1	System Architecture	B1	Security Feature User's Guide	B1
	Object Reuse	B1	System Integrity	B1	Trusted Facility Manual	B1
	Labels	B1	Security Testing	B1	Test Documentation	B1
	Label Integrity	B1	Design Specification and Verification	B1	Design Documentation	B1
	Exportation of Labeled Information	B1	Covert Channel Analysis	NR		
	Exportation to Multilevel Devices	B1	Trusted Facility Management	B2	**Accountability**	
	Exportation to Single-Level Devices	B1	Configuration Management	NR	Identification and Authentication	B1
	Labeling of Human-Readable Output	B1	Trusted Recovery	NR	Audit	B1
	Mandatory Access Control	NR	Trusted Distribution	NR	Trusted Path	B2
	Subject Sensitivity Labels	NR				
	Device Labels					

LEGEND: NA = Requirement is not applicable for this product; NR = No requirements for this class; C = Meets CMW requirements; W = Received CMW requirement waiver from DIA

PRODUCT: **INFORMIX-OnLine/Secure Release 5.0**

OVERALL RATING C2

VENDOR
Informix Software, Inc.

PLATFORMS
Multi-user, Multi-tasking UNIX Platforms

RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
Security Policy		**Assurance**		**Documentation**	
Discretionary Access Control	C2	System Architecture	B1	Security Feature User's Guide	C2
Object Reuse	C2	System Integrity	C2	Trusted Facility Manual	C2
Labels	NR	Security Testing	C2	Test Documentation	C2
Label Integrity	NR	Design Specification and Verification	NR	Design Documentation	C2
Exportation of Labeled Information	NR	Covert Channel Analysis	NR		
Exportation to Multilevel Devices	NR	Trusted Facility Management	NR	**Accountability**	
Exportation to Single-Level Devices	NR	Configuration Management	NR	Identification and Authentication	C2
Labeling of Human-Readable Output	NR	Trusted Recovery	NR	Audit	C2
Mandatory Access Control	NR	Trusted Distribution	NR	Trusted Path	NR
Subject Sensitivity Labels	NR				
Device Labels	NR				

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

PRODUCT: INFORMIX-OnLine/Secure

OVERALL RATING B1

VENDOR
Informix Siftware, Inc.

PLATFORMS

See Product Description

RATING CRITERIA	RATING	RATING CRITERIA	RATING	RATING CRITERIA	RATING
Security Policy		**Assurance**		**Documentation**	
Discretionary Access Control	C2	System Architecture	B1	Security Feature User's Guide	C2
Object Reuse	C2	System Integrity	B1	Trusted Facility Manual	B1
Labels	B1	Security Testing	B1	Test Documentation	C2
Label Integrity	B1	Design Specification and Verification	B1	Design Documentation	B1
Exportation of Labeled Information	B1	Covert Channel Analysis	NR		
Exportation to Multilevel Devices	B1	Trusted Facility Management	NR	**Accountability**	
Exportation to Single-Level Devices	B1	Configuration Management	NR	Identification and Authentication	B1
Labeling of Human-Readable Output	B1	Trusted Recovery	NR	Audit	B1
Mandatory Access Control	NR	Trusted Distribution	NR	Trusted Path	NR
Subject Sensitivity Labels	NR				
Device Labels					

LEGEND: NA = Requirement is not applicable for this product
C = Meets CMW requirements
NR = No requirements for this class
W = Received CMW requirement waiver from DIA

2.4 **Security Packages for MS-DOS Micros, Workstations, and Personal Computers**. Security officials, department heads, and supervisors face difficult security problems dealing with the thousands of micros, workstations, and personal computers used throughout the DON. On the one hand, meeting the mission with computers has become a way of life. Manual methods can simply no longer keep pace with information intense tasks. However, a computer in every work place or on every desk poses security risks. Industry has responded with security packages addressing those risks. While these packages sometimes appear to "solve your complete PC security problems," with but rare exceptions, none actually do. Thus, you need to use caution before you commit to reliance on claimed "protection" features.

a. Features. Most security packages available for micros, workstations, and personal computers target the MS-DOS class machine (i.e., IBM personal computers and compatibles). Their safeguards thus supplement, but do not replace, the elementary "protection" techniques offered by MS-DOS. Listing the safeguards you need can be an invaluable first step as you review candidate security packages and their capabilities. For example, audit trail recording features are invaluable for maintaining management oversight on a system's users and their activities while accessing the system.

b. Criteria. Since no available security package for MS-DOS based machines REPLACES the operating system itself with one having designed-in security features, no package can, by definition, meet TCSEC parameters for any but the default, Class D, Minimal Protection, criteria. In response to this dilemma, NCSC published its *Computer Security Subsystem Interpretation (CSSI) of the DoD Trusted Computer System Evaluation Criteria*, September 1988. The CSSI criteria and rating scheme follows TCSEC, as Figure 2.4-1 shows. As you review the evaluated security packages, you should keep in mind that a security feature rated as D3 is significantly "better" than the same feature rated at D1 for another security package.

c. Evaluated Security Packages for Micros, Workstations, and Personal Computers. The matrices also follow the alphabetical, by product, grouping scheme. In some instances, a Rated Criterion's "Rating" will be an "**X**" to indicate the criterion has been assessed, but not rated.

TCSEC vs. CSSI RATING SCHEME	
TCSEC Ratings	CSSI Ratings
D	D
C1	D1
C2	D2
B1	No Equivalent
B2	
B3	D3
A1	No Equivalent

Figure 2.4-1

MICROCOMPUTER SECURITY PRODUCTS

Product	Rated By	Overall Rating	Platform	Vendor	Rating Criteria	Rating
DR DOS 6.0 Microcomputer Operating System	**NISE EAST**	**None**	**Any IBM or compatible computer**	**Digital Research Corp.**	**Security Policy** Discretionary Access Controls Object Reuse	 X ---
					Accountability Identification and Authentication Audit	 X ---
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing	 X

					Trusted Facility Manual Test Documentation Design Documentation	X --- ---
Eyedentify Information Security System	**NCSC**	**I&A D1**	**Any System**	**Eyedentify Corporation**	**Security Policy** Discretionary Access Controls Object Reuse	 --- ---
					Accountability Identification and Authentication Audit	 D1 ---
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Desig Documentation	 --- --- --- ---

Product	Rated By	Overall Rating	Platform	Vendor	Rating Criteria	Rating
ISAC 2200 V 1.40	USAF-PERC	None	ZDS Z-150	Isolated Systems Limited	**Security Policy** Discrn etionary Access Controls Object Reuse	 X X
					Accountability Identification and Authentication Audit	 X X
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---

Product	Rated By	Overall Rating	Platform	Vendor	Rating Criteria	Rating
MAILSAFE Public Key Encryption	**USAF-PERC**	**None**	**ZDS Z-150 ZDS Z-184 ZDS Z-200 ZDS Z-248**	**Fisher Intn'l Systems Corporation**	**Security Policy** Discretionary Access Controls Object Reuse	 --- ---
					Accountability Identification and Authentication Audit	 X ---
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---

Product	Rated By	Overall Rating	Platform	Vendor	Rating Criteria	Rating
Micro Control	**NCSC**	**DAC D** **I&A D** **AUD D**	**Wang Pro Computer 200/300 Series**	**Wang Labs**	**Security Policy** Discretionary Access Controls Object Reuse	 D ---
					Accountability Identification and Authentication Audit	 D D
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---
ONGUARD 4.10	**NCSC**	**DAC D1** **I&A D1**	**IBM PC-XT** **IBM PC-AT** **or** **100% BIOS Compatibles**	**E-X-E Corporation**	**Security Policy** Discretionary Access Controls Object Reuse	 D1 ---
					Accountability Identification and Authentication Audit	 D1 ---
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---

Product	Rated By	Overall Rating	Platform	Vendor	Rating Criteria	Rating
PC/DACS	**NCSC**	**DAC D OR D I&A D AUD D**	**IBM PC-XT IBM PC-AT or 100% BIOS Compatibles**	**Pyramid Corporation**	**Security Policy** Discretionary Access Controls Object Reuse	 D D
					Accountability Identification and Authentication Audit	 D D
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---
SECUREPC	**USAF-PERC**	**None**	**ZDS Z-150 ZDS Z-184 ZDS Z-200 ZDS Z-248 ZDS Z-386**	**Hughes Data Systems**	**Security Policy** Discretionary Access Controls Object Reuse	 X X
					Accountability Identification and Authentication Audit	 X X
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---

Product	Rated By	Overall Rating	Platform	Vendor	Rating Criteria	Rating
Tigersafe	**NCSC**	**OR D I&A D**	**IBM PC-XT IBM PC-AT ZDS Z-248**	**The ALC Group**	**Security Policy** Discretionary Access Controls Object Reuse	 --- D
					Accountability Identification and Authentication Audit	 D ---
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---

Product	Rated By	Overall Rating	Platform	Vendor	Rating Criteria	Rating
Trispan	**NCSC**	**DAC D I&A D AUD D**	**IBM PC-XT IBM PC-AT**	**MICRONYX**	**Security Policy** Discretionary Access Controls Object Reuse	 D ---
					Accountability Identification and Authentication Audit	 D D
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---
Watchdog	**NCSC**	**DAC D2 OR D I&A D2 AUD D2**	**IBM PC-XT IBM PC-AT**	**Fisher Intn'l Systems Corporation**	**Security Policy** Discretionary Access Controls Object Reuse	 D2 D
					Accountability Identification and Authentication Audit	 D2 D2
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---

Product	Rated By	Overall Rating	Platform	Vendor	Rating Criteria	Rating
Watchdog	**USAF-PERC**	**None**	**IBM PC-XT IBM PC-AT**	**Fisher Intn'l Systems Corporation**	**Security Policy** Discretionary Access Controls Object Reuse	 X X
					Accountability Identification and Authentication Audit	 X X
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---

Product	Rated By	Overall Rating	Platform	Vendor	Rating Criteria	Rating
Watchdog Armor	**USAF-PERC**	**None**	**IBM PC-XT IBM PC-AT**	**Fisher Intn'l Systems Corporation**	**Security Policy** Discretionary Access Controls Object Reuse	 --- ---
					Accountability Identification and Authentication Audit	 --- X
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---
LOCKIT I Extended Edition Version 3.3	**USAF-PERC**	**None**	**IBM PS/2 & Clones**	**Security Microsystems, Inc.**	**Security Policy** Discretionary Access Controls Object Reuse	 X ---
					Accountability Identification and Authentication Audit	 X X
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---

Product	Rated By	Overall Rating	Platform	Vendor	Rating Criteria	Rating
LOCKIT PROFESSIONAL	**USAF-PERC**	**None**	**IBM PS/2 & Clones**	**Security Microsystems, Inc.**	**Security Policy** Discretionary Access Controls Object Reuse	 X X
					Accountability Identification and Authentication Audit	 X X
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---

Product	Rated By	Overall Rating	Platform	Vendor	Rating Criteria	Rating
RAMPART-PC Menu System Version 3.03	**USAF-PERC**	**None**	**IBM & compatible**	**Breakpoint Software, Inc.**	**Security Policy** Discretionary Access Controls Object Reuse	 X X
					Accountability Identification and Authentication Audit	 X X
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---
Secure PC and Secure PC PLUS Version 5.0	**USAF-PERC**	**None**	**Not Available**	**Hughes Data Systems**	**Security Policy** Discretionary Access Controls Object Reuse	 X X
					Accountability Identification and Authentication Audit	 X X
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---

Product	Rated By	Overall Rating	Platform	Vendor	Rating Criteria	Rating
V-PHAGE Version 2.1	**USAF-PERC**	**None**	**IBM & Compatibles**	**Application Configuration Computers, Inc.**	**Security Policy** **Discretionary Access Controls** **Object Reuse**	 **X** **X**
					Accountability Identification and Authentication Audit	 X X
					Assurance Architecture System Integrity Security Testing	 --- --- ---
					Documentation Security Features Testing Trusted Facility Manual Test Documentation Design Documentation	 --- --- --- ---

2.5 **Assessed Overwrite Tools**. These tools implement the Magnetic Remanence safeguard feature described in the Remanence Overwrite Criteria publications indicated below in Figure 2.5-1. As prescribed, the tools provide assurance that, when overwritten, sensitive or classified information recorded on a storage device (disk or diskette) cannot be subsequently read, copied, or otherwise recovered by an unauthorized person.

a. Features. Two features are important: clearing and purging.

■ Clearing is sufficient when the media will continue to have positive administrative security procedures applied and will remain within a controlled, physically secure space.

■ Purging is mandatory when administrative and physical controls will no longer be applied (e.g., a hard disk equipped Z-248 will be transferred to another activity).

b. Criteria. Overwrite assessment criteria have been published by several organizations, as the Figure 2.5-1 indicates. The algorithms which perform clear or purge overwrite functions must follow the steps shown in Figure 2.5-2.

REMANENCE OVERWRITE CRITERIA	
Organization	Publication
National Computer Security Center	DoD Magnetic Remanence Security Guideline, CSC-STD-005-85, 15 November 1985. [CSC-STD]
Department of the Navy	Department of the Navy Automatic Data Processing Security Program, OPNAVINST 5239.1A, August 1982. [OPNAV]
Naval Electronic Systems Security Engineering Center	Automated Information Systems Remanence Security Guidebook, NISE EAST 5239.1-G, 19 September 1990. [AISRG]

Figure 2.5-1

Overwrite Mode	MINIMUM DISK OVERWRITE REQUIREMENTS				
	Operation Performed		AIS RSG	CSC STD	OP NAV
Purge	1.	Write any character, then its complement, alternating each 3 times.	X	X	--
		Write binary ones, then binary zeros, alternating each 3 times.	--	--	X
	2.	Write any last character once.	X	X	X
	3.	Verify and retain last written character.	X	X	X
Clear	1.	Write any character once.	X	X	X
	2.	Verify and retain written character.	X	X	X

Figure 2.5-2

c. Assessed Overwrite Tool Matrices. For additional information about these tools, see the alphabetically ordered executive summaries given in Chapter 3.

PRODUCT:	DeClass PC and FileZero PC	RATED BY: USAF		
	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
VENDOR OITC, Inc.	ZDS Z-150, ZDS Z-184, ZDS Z-200, ZDS Z-248, ZDS Z-386, IBM PS/2, Wang PC 282/382, COMPAQ SLT 286, COMPAQ 386, UNISYS Desktop III	Clear Purge	No No	--- ---
PRODUCT:	MacTools Deluxe	RATED BY: NISE EAST		
	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
VENDOR Central Point Software	Macintosh Plus	Clear Purge	No No	No No
PRODUCT:	Mace Utilities V1990.1 DESTROY FILE	RATED BY: NISE EAST		
	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
VENDOR Fifth Generation	ZDS Z-150, ZEOS 386SX	Clear Purge	No No	No No

PRODUCT:	DECLASFY Version2.05.12	RATED BY: USAF-PERC		
VENDOR Mr Dan Mares	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
	IBM and Compatibles			
PRODUCT:	Norton Utilities V 4.01 WIPEFILE & WIPEDISK	RATED BY: USAF-PERC		
VENDOR Symantec	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
	ZDS Z-150, ZDS Z-184, ZDS Z-200, ZDS Z-248	Clear Purge	Yes Yes	--- ---
PRODUCT:	Norton Utilities WipeInfo and DECLASFY V 5.0 & 6.0	RATED BY: USAF-PERC		
VENDOR Symantec	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
	IBM and Compatibles			

PRODUCT:	Norton Utilities Advanced Edition 4.5 WIPEFILE & WIPEDISK	RATED BY: USAF-PERC		
	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
VENDOR Symantec	ZDS Z-150, ZDS Z-184, ZDS Z-200, ZDS Z-248, TEMPEST z-248, COMPAQ 386, Sperry 3070, UNISYS Desktop III, (MS-DOS 3.1 or earlier)	Clear Purge	Yes Yes	--- ---

PRODUCT:	Norton Utilities V 5.0 WIPEINFO	RATED BY: NISE EAST		
	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
VENDOR Symantec	ZDS Z-150, ZDS Z-184, ZDS Z-200, ZDS Z-248, (MS-DOS 3.1 or earlier)	Clear Purge	Yes Yes	Yes Yes

PRODUCT:	Overwrite Program to Declassify Floppy or Hard Disk (KILLDISK) V 3.0 & 4.0	RATED BY: USAF-PERC		
	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
VENDOR Pan American	ZDS Z-148, ZDS Z-150, ZDS Z-248, ZEROS 386SX-16	Clear Purge	Partial ---	--- ---

PRODUCT:	Overwrite Program to Declassify Floppy or awrd Disk (KILLDISK) V 5.0	RATED BY: USAF-PERC		
	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
VENDOR Pan American	ZDS Z-148, ZDS Z-150, ZDS Z-248, TEMPEST Z-248, ZEOS 386SX-16, COMPAQ 386, Sperry 3070, UNISYS Desktop III	Clear Purge	Partial Partial	--- ---

PRODUCT:	PC Tools Deluxe V 6 CLEAR FILE	RATED BY: NISE EAST		
	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
VENDOR Central Point Software	ZDS Z-148, ZDS Z-150, ZDS Z-248, ZEOS 386SX-16	Clear Purge	Yes No	Yes No

PRODUCT:	PC Tools V 7 WIPE	RATED BY: NISE EAST		
	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
VENDOR Central Point Software	ZDS Z-148, ZDS Z-150, ZDS Z-248, ZEOS 386SX-16	Clear Purge	Yes Yes	Yes Yes

PRODUCT:	PRIAM Hard Disk Formatting Software Programs V 4.02	RATED BY: USAF-PERC		
	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
VENDOR PRIAM Systems Division	TEMPEST Z-248		No No	--- ---

PRODUCT:	Sanitization Software for the AT&T 3B2/600G V 1.1.0	RATED BY: USAF-PERC		
	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
VENDOR AT&T	AT&T 3B2		Yes No	--- ---

PRODUCT:	SGT Security Version 4A	RATED BY: NCSC		
	PLATFORMS	RATED CRITERIA	RATING	CSC-STD-005-85 Compliance
VENDOR Pike Creek Computers	IBM PC/XT, IBM AT		Yes Yes	--- ---

2.6 **Assessed Trusted Applications**. These specialized products use a security protection strategy which reverses the roles normally found in secure AISs. Here, the application itself implements needed security safeguard features, while the operating system provides "reliable functions" or services, not trusted ones. Accordingly, trusted applications must be used in a physically secure environment so that no unauthorized person can use operating system commands or features to circumvent the applications-enforced safeguards (e.g., the Dedicated Security Mode is appropriate).

a. Features. While trusted applications do not have a common theme for their functionality, their implemented security safeguards parallel those found in Add-On Security Packages. Please refer to Section 2.4, above.

b. Criteria. NCSC's *CSSI*, described earlier, is appropriate for assessing the security safeguards found in trusted applications. Please refer to Section 2.4b, above.

c. Assessed Trusted Applications Matrices. For additional information about Assessed Trusted Applications, see alphabetically arranged executive summaries.

ASSESSED TRUSTED APPLICATIONS

Product	Rated By	Overall Rating	Platform	Vendor	Rating Criteria	Rating
Secure Electronic Bulletin Board System (SEBBS)	**NISE EAST**	**D2**	**ZDS Z-248** **AT&T STU-III (with SACS)** **MS-DOS 3.3 only**	**NAVELEX SECCEN**	**Security Policy** Discretionary Access Controls Object Reuse	 D3 D2
					Accountability Identification and Authentication Audit	 D3 D3
					Assurance Architecture System Integrity Security Testing	 D2 D2 D3
					Documentation Security Features Testing Trusted Facility Manual Test Documentation	 D3 D3 D3

2.7 **Other Assessed Security Products**. There are several other security products that can provide protection mechanisms for specific circumstances. If you have a similar situation, you should consider using these available products, rather than developing one.

a. Features. Since these products have no common security protection theme, you need to consult the individual assessment executive summaries.

b. Criteria. There are no formal assessment criteria published for these products. Rather, the functionality statement explicitly contains the assessment metric(s).

c. Other Assessed Security Products Matrices. For additional information about these products, consult the alphabetically arranged executive summaries in Chapter 3.

OTHER ASSESSED PRODUCTS

PRODUCT:	Disinfect Version 2.5.1	RATED BY: USAF-PERC	
VENDOR USAF	PLATFORMS	RATED CRITERIA	RATING
	Not Available	Assurance System Integrity	X
PRODUCT:	Modified Hard Disk Control Cable	RATED BY: USAF-PERC	
VENDOR USAF	PLATFORMS	RATED CRITERIA	
	ZDS Z-248	Assurance System Integrity	X
PRODUCT:	NoFBoot and SumFBoot	RATED BY: USAF-PERC	
VENDOR a. Padget Peterson	PLATFORMS	RATED CRITERIA	RATING
	ZDS Z-248	Assurance System Integrity	X

OTHER ASSESSED PRODUCTS

PRODUCT:	Norton Commander Version 2.0	RATED BY: USAF-PERC	
	PLATFORMS	RATED CRITERIA	RATING
VENDOR Symantec	ZDS Z-150, ZDS Z-184, ZDS Z-200, ZDS Z-248	Assurance System Integrity	X

PRODUCT:	Norton Utilities Programs Version 5.0	RATED BY: USAF-PERC	
	PLATFORMS	RATED CRITERIA	RATING
VENDOR Symantec	Not Available	Assurance System Integrity	X

PRODUCT:	NoZFBoot V 1.0	RATED BY: NISE EAST	
	PLATFORMS	RATED CRITERIA	RATING
VENDOR NISE EAST	ZDS Z-248	Assurance System Integrity	X

OTHER ASSESSED PRODUCTS

PRODUCT:	ODCSOPS Security Format (FILLDISK)	RATED BY: USAF-PERC	
VENDOR USAF	PLATFORMS	RATED CRITERIA	RATING
	ZDS Z-184, ZDS Z-248, UNISYS Desktop III	Assurance System Integrity	X
PRODUCT:	PC secure Version 1.0	RATED BY: USAF-PERC	
VENDOR USAF	PLATFORMS	RATED CRITERIA	RATING
	ZDS Z-150, ZDS Z-184, ZDS Z-200, ZDS Z-248, ZDS Z386, IBM PS/2, Wang PC-280, Wang PC-382, COMPAQ SLT 286, COMPAQ 386, UNISYS Desktop III	Assurance System Integrity	X
PRODUCT:	Personal Computer Security System	RATED BY: USAF-PERC	
VENDOR Media Security Corporation	PLATFORMS	RATED CRITERIA	RATING
	Not Available	Assurance System Integrity	X

OTHER ASSESSED PRODUCTS

PRODUCT:	SECURECOPY	RATED BY: USAF-PERC	
VENDOR USAF	PLATFORMS	RATED CRITERIA	RATING
	Not Available	Assurance System Integrity	X

PRODUCT:	VirHUNT	RATED BY: USAF-PERC	
VENDOR Digital Dispatch, Inc.	PLATFORMS	RATED CRITERIA	RATING
	Not Available	Assurance System Integrity	X

PRODUCT:	VIRUSCAN Version 6.3V72	RATED BY: USAF-PERC	
VENDOR McAfee Associates	PLATFORMS	RATED CRITERIA	RATING
	Not Available	Assurance System Integrity	X

OTHER ASSESSED PRODUCTS

PRODUCT: VSHIELD Version 3.4V79		RATED BY: USAF-PERC	
	PLATFORMS	RATED CRITERIA	RATING
VENDOR McAfee Associates	Not Available	Assurance System Integrity	X

Chapter 3

ASSESSED PRODUCTS

The following executive summaries provide information for those products assessed under U.S. Navy (NISE EAST) and U.S. Air Force (USAF-PERC) auspices. For additional information, please contact:

Naval Command, Control and Ocean Surveillance Center In Service Engineering
(NISE EAST)
Code 043
4600 Marriott Drive
North Charleston, SC. 29406-6504

DSN 292-0738

Commercial (202) 282-0738

THIS PAGE INTENTIONALLY BLANK

3.1 DOS SECURITY PRODUCTS

ASSESSED PRODUCT: DECLASFY
VENDOR: Mr Dan Mares
VERSION: 2.05.12
FINAL USAF-PERC ASSESSMENT REPORT: 90-502 23 June 1991
PRODUCT DESCRIPTION:

DECLASFY Version 2.05.12 is a program to declassify hard disks on International business Machines (IBMs) and compatible personal computers. The program is designed to meet Department of Defence (DOD) standards concerning declassification of hard disks. The DOD standard requires declassifying hard disks using the following procedures: write a character (such as binary 0) to every addressable location, then write its compliment (binary 1) to every addressable location. After at least three overwrite cycles, write a random character to all locations, thus giving a total of seven overwrites. In addition to the seven overwrites, DECLASFY makes two more overwrite passes giving a combined total of nine overwrites. Also, DECLASFY can be used to **clear** floppy disks by overwriting all addressable locations at least one time with one overwrite cycle.

ASSESSMENT SUMMARY:

DECLASFY meets the criteria outlines in AFSSI 5020 for declassifying hard disks and clearing floppy disks. DECLASFY and all of its options were found to function properly as stated in the program documentation.

DECLASFY did not recognize the external floppy drive on the IBM PS/2 models 50 and 70 computers. Do not use DECLASFY to clear a floppy disk or diskette on an external drive that is not physically recognized by the disk controller as being drive A: or B:. Also, DECLASFY only recognized the first two physical hard drives on a computer configuration. **NOTE:** DECLASFY **does not** recognize logical (partition) drives. It only recognizes physical drives.

RECOMMENDATIONS:

Users should execute the DECLASFY program without any options o ensure compliance with DOD standards.

When a user encounters an error, recommend the user verify that there is no classified or readable data in that sector where the error occurred. Also, if any errors occur while overwriting, or if any unusable sector/track could not be overwritten, recommend using an approved degausser to purge the data from the hard disk. Do not use DECLASFY to overwrite any drives that are not physically recognized by the disk controller.

After executing DECLASFY on the Zenith 248 and 386 computers hard disks, users should verify there is no residual data residing in the last track of the hard disks.

ASSESSED PRODUCT: DeClass PC and FileZero PC
VENDOR: OITC, Incorporated
VERSION: N/A
FINAL USAF-PERC ASSESSMENT REPORT: 90-511 5 June 1991
PRODUCT DESCRIPTION:

The DeClass PC and FileZero PC are programs designed to meet the needs of IBM PC and PC compatible users who are using their PCs to process national security information. DeClass PC and FileZero PC support classified data processing users and those users who must use the same equipment in both a classified and an unclassified environment. DeClass PC provides for the declassification of main memory, video memory, miscellaneous memory within the address range of hex A0000 to FFFFF, floppy disks, hard drives, and printer buffers. Four levels of declassification provided are: Company Private, Confidential, Secret and Top Secret. Company Private is used for the protection of sensitive but unclassified data, information covered by the privacy act, proprietary data, etc.

Disks are declassified by writing all binary ones to every sector on the disk followed by a write of binary zeros to every sector. A final write of the character "?" is accomplished following the write of binary zeros. The "?" character can be changed by the user as a function of the DeClass PC Environment Setup Option. Upon completion of the final write cycle, DeClass PC calculates twenty random sector addresses and then verifies that these sectors contain only the selected final overwrite character.

Declassifying of the printer is accomplished by the output of twice the number of bytes provided for in the printer's buffer as specified during the system environment session. This memory size value is then overwritten appropriately for the declassification level.

All semiconductor memory is declassified by cycling between an all binary ones state and an all binary zeros state 100 times for Confidential or Secret data and 1000 times for Top Secret data. Company Private or sensitive but unclassified data is overwritten only once.

File Zero PC is a collection of utility programs intended for the declassification of specific files, free memory areas, and the ends of existing files. The File Zero PC utility programs consist of:

- o FILE0.COM - Used to declassify individual files.
- o CLRFREE.EXE - Used to declassify all free memory areas as well as the ends of files that are to remain on disk.
- o CHEKEOF.EXE - Used to verify that the end of each file resident on disk does not contain classified data.
- o SCANDISK.EXE - Used to scan the entire contents of the user/program accessible disk storage area.

ASSESSMENT SUMMARY:

Although the DeClass PC and FileZero PC programs were considered to be a security subsystem rather than a complete trusted computer system, they were assessed against the requirements for object reuse in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985, AFR 205-16, 28 April 1989, and the Security Guideline (MRSG), 15 November 1985, and Air Force Systems Security Instruction (AFSSI) 5020 Remanence Security, 15 April 1991.

The Declassification of Floppy Drives program **DID NOT** function on any of the following test configurations:

- Z-150 with one 5.25-inch 360 KB floppy drive (drives A: or B:)
- Z-200 with two 5.25-inch 360 KB floppy drives (drives A: or B:)
- Z-248 with two 5.25-inch 360 KB floppy drives (drives A: or B:)
- Z-248 with one 5.25-inch 360 KB floppy drive (drive A:), one 5.25-inch 1.2 MB floppy drive (drive B:)
- Z-386 with two 5.25-inch 360 KB floppy drives (drives A: or B:)
- Z-184 with one 3.5-inch 720 KB floppy drive (drives A: or B:)
- IBM PS/2 Model 30 with one 3.5-inch 1.44 MB floppy drive (drive A:), and one 5.25-inch 360 KB external floppy drive (drive B:)
- IBM PS/2 Model 50 with one 3.5-inch 1.44M floppy drive (drives A: or B:)
- IBM PS/2 Model 70 with one 3.5-inch 1.44M floppy drive (drives A: or B:)
- Wang PC 282/20 with one 5.25-inch 1.2M floppy drive (drives A: or B:)
- Wang PC 382 with one 5.25-inch 1.2M floppy drive (drives A: or B:)
- COMPAQ SLT 286 laptop with one 3.5-inch 1.44M floppy drive (drive A:) and one external 5.25-inch 1.2M external floppy drive (drive B:)

- o COMPAQ Deskpro 386/25 with one 5.25-inch 1.2M floppy drive (drive A:) and one 3.5-inch 1.44M floppy drive (drive B:)

- o UNISYS Desktop III PW/2 800/16 with one 3.5-inch 1.44M floppy drive (drive A:) and one 5.25-inch 360 KB floppy drive (drive B:)

- o UNISYS Desktop III PW/2 800/20C with one 3.5-inch 1.44M floppy drives (drive A:) and one 5.25-inch 360 KB floppy drive (drive B:)

Declassification of Hard Disks **DID NOT** function on the following test configurations:

- o Zenith Z-150 with external hard drives

- o Zenith Z-386 with 53 MB removable hard disk partitioned at 32 MB and 20 MB (drives C: and D:) and one 10 MB removable hard disk (drive E:)

- o IBM PS/2 Model 50 with 60 MB nonremovable hard disk partitioned at 40 MB and 20 MB (drives C: and D:)

- o IBM PS/2 Model 70 with 120 MB nonremovable hard disk partitioned at 35 MB, 20 MB, 20 MB, 20 MB, and 20 MB (drives C:, D:, E:, and F:)

- o Wang PC 280/20 with 41 MB nonremovable hard disk partitioned at 25 MB and 16 MB (drives C: and D:)

- o UNISYS Desktop III PW/2 800/16 with 320 MB nonremovable disk partitioned at 100 MB, 100 MB, 60 MB, and 60 MB (drives C:, D:, E:, and F:)

- o UNISYS Desktop III PW/2 800/20C with 42 MB removable Bernoulli cartridge disk partitioned at 30 MB and 12 MB (drives C: and D:)

- o UNISYS Desktop III PW/2 800/20C with 320 MB nonremovable hard disk partitioned at 100 MB, 100 MB, 60 MB, and 60 MB (drives C:, D:, E:, and F:)

Declassification of Random Access Memory (RAM) **DID NOT** function on the following test configurations:

- o Zenith Z-150 with 640K DOS Memory
- o Zenith Z-248 with 640K DOS Memory and 256K Extended Memory
- o Zenith Z-248 with 640K DOS Memory
- o Zenith Z-386 with 640K DOS, 1 MB Extended Memory, and 3 MB Expanded Memory

Declassification of Printer Memory program functioned on all of the test configurations.

DO NOT use CLRFREE.EXE on any **HARD DISKS** of the following test configurations.

- o Z-150 with one 10 MB removable hard disk (drive C:) and two external 10 MB removable hard disks (drives D: and E:)
- o Z-200 with two 10 MB removable hard disks (drives C: and D:)
- o Z-248 with one 20 MB nonremovable hard disk (drive C:) and one 40 MB nonremovable hard disk (drive D:)
- o Z-248 with one 40 MB nonremovable hard disk (drive C:)
- o Z-386 with one 53 MB removable hard disk partitioned at 32 MB and 21 MB (drives C: and D:) and one 10 MB removable hard disk (drive E:)
- o Z-184 laptop with one 20 MB nonremovable hard disk (drive C:)
- o IBM PS/2 Model 30 with one 20 MB removable hard disk (drive C:)
- o IBM PS/2 Model 50 with one 60 MB nonremovable hard disk partitioned at 40 MB and 20 MB (drives C: and D:)
- o IBM PS/2 Model 70 with one 120 MB nonremovable hard disk partitioned at 40 MB, 20 MB, 20 MB, 20 MB, and 20 MB (drives C:, D:, E:, F:, and G:), and one 5.25-inch 1.2 MB external floppy drive (drive H:)
- o Wang PC 282/20 with one 41 MB nonremovable hard disk partitioned at 25 MB and 16 MB (drives C: and D:)
- o Wang PC 382 with one 70 MB nonremovable hard disk partitioned at 32 MB, 19 MB and 19 MB (drives C:, D:, and E:)
- o COMPAQ SLT 286 laptop with one 20 MB nonremovable hard disk (drive C:)
- o COMPAQ Deskpro 386/25 with one 300 MB nonremovable hard disk partitioned at 100 MB, 50 MB, 50 MB, 50 MB, and 50 MB (drives C:, D:, E:, and F:)
- o UNISYS Desktop III PW/2 800/16 with one 320 MB nonremovable hard disk partitioned at 100 MB, 100 MB, 60 MB, and 60 MB (drives C:, D:, E:, and F:)
- o UNISYS Desktop III PW/2 800/20C with one 42 MB removable Bernoulli cartridge disk partitioned at 30 MB and 12 MB (drives C: and D:)

Z **DO NOT** use SCANDISK.EXE or CHEKEOF.EXE on any of the test configurations. Utilities such as Norton Utilities, PCTOOLS, or MACE should be used for verification of erasure of data and files and unused portions of floppy drives and hard disks.

Use CLRFREE.EXE and FILE0.COM on **FLOPPY DRIVES ONLY** of the test configurations. Utilities such as Norton Utilities, PCTOOLS, or MACE should be used for verification of erasure of data and files and unused portions of floppy drives.

NOTE:

The Macintosh DeClass version 2.2, which operates only on version 4.2 of the Macintosh Operating System, was not assessed. This version will not execute under version 6.0 or greater of the Macintosh Operating System.

ASSESSED PRODUCT: DR DOS 6.0 Microcomputer Operating System

VENDOR: Digital Research Corporation

VERSION: 6.0

DATE: 12 December 1991

FINAL NISE EAST ASSESSMENT REPORT: No report number assigned

PRODUCT DESCRIPTION:

Distributed by Digital Research Corporation, DR DOS 6.0 is an alternative operating system for IBM compatible microcomputers. While it contains features similar to MS-DOS Version 5.0, DR DOS 6.0 replaces many traditional "DOS" functions and programs with ones having enhanced functionality. For example, COMMAND.COM, CHKDSK.COM, and several other "standard" routines have their unique implementation under DR DOS 6.0. DR DOS 6.0 also includes certain "security safeguards" not present in either MS-DOS or PC-DOS. Thus, a System Administrator can, for a single- or multi-user environment, enable or disable all security safeguards as well as selectively determine which file(s) (e.g., programs, data) or subdirectory(ies) will have a graduated protection scheme applied (e.g., read, write, or delete) via password(s). When used per the documentation, DR DOS 6.0 claims:

> "DR DOS offers an option to secure your entire operating system. When you choose the system security option during INSTALL, or at any later time when you run SETUP, you can specify two levels of password-protection; that is, one of the passwords must be typed in by the user in order to gain access to DR DOS on your computer. This protects your data, and your fixed disks, by preventing unauthorized access to them."

ASSESSMENT SUMMARY:

DR DOS 6.0 claims to implement certain elementary system-enforced safeguard features and capabilities analogous to the Identification and Authentication (I&A) mechanisms and Discretionary Access Control (DAC) mechanisms described in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), December 1985. Since DR DOS 6.0 does not implement Object Reuse or Audit Trail features, it is appropriate to use the least trustworthy criteria set, Discretionary Access Protection, or Class C1, for its assessment.

During DR DOS 6.0 installation, a System Administrator can optionally select to enable or ignore the security features inherent in its design (it can be successfully installed and used without invoking its optional security features). If security features will be used, I&A features require the System Administrator, or Master Key Password Holder, to establish and configure the system's security features via menu driven dialogue. In doing so, the Master Key Password Holder registers himself or herself with the system, assigns the one

permitted User Key Password, and determines which files and/or subdirectories will have which protection level(s) applied via specific password(s).

Thereafter, before the system completes its initialization (e.g., invokes CONFIG.SYS or AUTOEXEC.BAT), the I&A features require a candidate user to log-on using either of two principal password modes: Master Key Password Holder or User Key Password Holder. Then, depending on whether or not files or subdirectories have graduated (i.e., increasingly privileged) password protection applied independently of either log-on password(s), the system denies or grants access accordingly, see Table 1.

OPTION	PERMITTED ACTION WITHOUT PASSWORD and FULL READ, WRITE, AND DELETE PROTECTION INVOKED							
	Protection Level(s)	Mask Used	Read From	Write To	Delete	Copy	Rename	Change Attributes
/R:password [READ]	R W D	DD0D	No	No	No	No	No	No
/W:password [WRITE]	R W	5505	Yes	No	No	Yes	No	No
/D:password [DELETE]	D	1101	Yes	Yes	No	Yes	No	No

Table 1

When configured and used according to the provided documentation, DR DOS 6.0 provides effective, but elementary, barriers against many security-related risks inherent in traditional "MS-DOS" class microcomputers. Specifically, DR DOS 6.0 implements:

- Identification and Authentication Features:

-- Its basic log-on I&A feature checks restrict powerful security enabling and disabling privileges to the Master Key Password Holder ONLY.

-- The single permitted User Key Password check at log-on deters unauthorized system access, but the password's wide-spread knowledge among all successful candidate users dilutes its I&A effectiveness.

- Discretionary Access Control Features:

-- Graduated (i.e., increasingly privileged) DAC-enforced checks can be readily tailored to meet specific security-constrained configuration requirements in a multi-user environment. For example, the System Administrator can provide effective restraints per the rules illustrated in Table 1, allowing, for example, "read from" file, but not "write to" file privileges. See also Table 2 for illustrative results achieved during testing.

-- Protection against circumventing the security environment by booting from a floppy diskette and then accessing the hard drive effectively thwarts many malicious acts.

■ Documentation:

-- Trusted Facility Manual. Digital Research incorporates an overview and some basic detail about its protection strategy in Chapter 4, DR DOS User Guide.

-- Security Features User's Guide. In addition to the information contained in the DR DOS User Guide, other useful information can be found in Chapter 9, Passwords, ViewMAX User Guide, to assist the user and/or System Administrator.

CAUTIONS AND PRECAUTIONS

■ Notwithstanding its modest security protection safeguards, DR DOS 6.0 can be readily rendered ineffective. During assessment testing, DR DOS 6.0 security was summarily defeated in its entirety as were all individual safeguards protecting either files or subdirectories. It was even possible to nullify its safeguard against loading from floppy diskette and then accessing the hard disk. Accordingly, System Administrators need to provide adequate physical protection and ruthlessly restrict powerful utility programs, as discussed in the documentation, to minimize these and other associated risks.

■ During functionality testing with WordPerfect and other applications, some anomalous "errors" were encountered. For example, WordPerfect's automatic "back-up" feature reported "File Creation Error" since the file in question could not be successfully renamed due to file protection having been invoked. System Administrators should, therefore, ***experiment extensively*** with their planned DR DOS 6.0 configuration and applications suite <u>before</u> committing to operational use.

■ Exporting diskette-based data files created and protected via DR DOS 6.0 may result in unexpected data "loss" in that the "hidden bit" may be set thus precluding a file from appearing in an MS-DOS directory listing on some other machine.

■ System Administrators must also understand that DR DOS 6.0 does not provide the minimum protection required for all DoD systems, i.e., Controlled Access Protection, Class C2.

Therefore, DR DOS 6.0 alone **MAY NEVER BE USED** as adequate protection for unclassified sensitive or classified information in DoD multi-user microcomputer environments.

DR DOS 6.0 ACCESS ATTEMPT RESULTS FOR PASSWORD PROTECTED FILES				
Attempted Act	Results When User DOES NOT Know the Associated Password and Full READ, WRITE, and DELETE Protection Has Been Applied			Remarks
	READ	WRITE	DELETE	
Read the File	NO	Yes	Yes	
Edit the File	NO	NO	Yes	
Delete the File	NO	NO	NO	
Rename the File	NO	NO	NO	
Change File Attributes	NO	NO	NO	
Copy the File	NO	Yes	Yes	
Type the File	NO	Yes	Yes	
Erase the File	NO	NO	NO	
Change File Name from Within an Application	NO	Yes	Yes	QEDIT
	NO	NO	NO	WordPerfect
Overwrite the File from Within an Application (Periodic Save)	NO	NO	NO	QEDIT
	NO	NO	NO	WordPerfect
Print via PRINT	NO	Yes	Yes	
XCOPY the File	NO	Yes	Yes	The copy has the "hidden" bit set
XDEL the File	NO	NO	Yes	
DELQ the File	NO	NO	NO	
Move the File	NO	NO	NO	

ASSESSED PRODUCT: Isolation System Access Control 2200 (ISAC 2200)

VENDOR: Isolation Systems Limited

VERSION: 1.40

DATE: July through September 1988

FINAL USAF-PERC ASSESSMENT REPORT: 88-501 10 November 1988

PRODUCT DESCRIPTION:

Isolation Systems Limited ISAC-2200 is a complete, self-contained data security system which controls access to the microcomputer. ISAC-2200 provides user Identification and Authentication (I&A), Discretionary Access Control (DAC) on objects, DAC on system resources (RAC), object reuse, and audit. Some of the additional security functions provided by ISAC-2200 are: peripheral device activity monitoring and control, tamper detection and reporting which consists of password tampering, device activity tampering, ISAC-2200 card removal from the microcomputer, battery removal tampering, cover removal tampering and zeroing of stored parameters on the ISAC-2200 board. ISAC-2200 is comprised of an expansion board and supporting software utilities. The expansion board itself provides all of the security mechanisms. The software utilities provide the ability to alter the specific characteristics of the security mechanisms. A management program is provided to access the ISAC-2200 configuration data such as user profiles and general system security parameters.

ASSESSMENT SUMMARY:

Since ISAC-2200 is considered to be a security subsystem rather than a complete trusted computer system, it was assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes I&A, DAC, object reuse, and audit. In addition, ISAC-2200 was assessed against the overwrite procedures outlined in the Department of Defense Magnetic Remanence Security Guideline (MRSG), 15 November 1985.

The ISAC-2200, when configured as tested on the Zenith Data Systems Z-150, does effectively implement the security mechanisms. In addition to the TCSEC features, ISAC-2200 was found to effectively implement the tampering detection mechanism. However, ISAC-2200 does not provide an object reuse mechanism to satisfy class C2 assurances described in the TCSEC and MRSG.

ASSESSED PRODUCT: LOCKIT I Extended Edition

VENDOR: Security Microsystems, Inc.

VERSION: 3.3

FINAL USAF-PERC ASSESSMENT REPORT: 91-504B 14 May 1992

PRODUCT DESCRIPTION:

LOCKIT I Extended Edition (LOCKIT) is a software security package designed to protect computer resources stored on the hard disk. LOCKIT is intended for use on IBM Personal System /2 computers and clones using PC-DOS or MS-DOS operating systems. The computer operating system files, application programs, data files, spread sheets, and documents, are resources protected from unauthorized access through LOCKIT's Discretionary Access Control (DAC), Identification and Authentication (I&A), and Audit mechanisms.

The System Administrator (SA - also known as LOCKIT Administrator) can grant access privileges on the computer by selecting options from a set of menus and tables found in LOCKIT.

ASSESSMENT SUMMARY:

Booting from a bootable floppy disk and using Norton Utilities allows users to circumvent the "MAXIMUM floppy boot protection" feature and I&A, DAC, and Audit mechanisms.

The option "ALL users may exit Lunch-Break" can lead to a violation of DAC privileges and should not be selected.

"The Hard Disk Abs I/O" option should check "-----" in the "Directory Access Control Table" to prevent Norton Utilities from absolute sector read and write to the hard disk. This option will only work after a valid logon. When the computer boots from the floppy drive, this feature cannot stop Norton Utilities.

Invalid logon attempts that occurred during the I&A (LOCKIT menus and tables) procedure cannot be recorded.

When the hard disk is full, audit information can be lost.

It is possible to lose some Audit information stored in RAM, if the "FLUSHLOG" command in not executed before the system is powered off.

The ".COM,.EXE Files" protection feature will not stop the DOS "DEL command from deleting files with ".EXE" and ".COM" extensions. Also, the DOS command "RENAME" can rename a non ".EXE" or ".COM" file to a ".EXE" or ".COM" file name.

RECOMMENDATIONS:

After LOCKIT has been installed, the floppy drive should be disabled. Disabling the floppy drive will prevent unauthorized hard disk access during a floppy boot up.

Do not store "LOCKIT.EXE" on the hard drive since this file has all the security options contained in the LOCKIT menus and tables. It will be necessary to turn off the password aging feature since this feature requires that "LOCKIT.EXE" be stored on the hard disk.

ASSESSED PRODUCT: LOCKIT PROFESSIONAL

VENDOR: Security Microsystems, Inc.

VERSION: 2.14

FINAL USAF-PERC ASSESSMENT REPORT: 91-504A 3 August 1992

PRODUCT DESCRIPTION:

LOCKIT PROFESSIONAL (LOCKIT) is a software and circuit board security package designed to protect computer resources stored on Personal Computers (PC). LOCKIT is intended for use on IBM Personal system/2 computers and clones using MS/PC-DOS operating systems 2.0 or greater. The LOCKIT circuit board will fit into any PC with Industry Standard Architecture (ISA) or Extended Industry Standard Architecture (EISA) but not the Micro Channel Architecture (MCA). The circuit board has Random Access Memory (RAM) and clock, both of which are powered by a lithium battery. The LOCKIT RAM contains executable logon code which contains part of LOCKIT's Identification and Authentication (I&A) mechanism. The I&A procedure begins before the bootstrap loader system calls are invoked and before MS/PC-DOS is loaded to the system's memory.

ASSESSMENT SUMMARY:

I&A. LOCKIT's I&A mechanism successfully prevents circumvention for all tested platforms, except for the IBM PS/2 model 20 and the UNISYS Desktop III PW/2 800/20C configured with a 42=MB removable Bernoulli cartridge. There is no limit to the number of logon attempts made during Lunch-Break.

DAC. When the boot protection mechanism fails, the DAC mechanism can be bypassed. The boot protection mechanism can be bypassed with the UNISYS. Wang, and Zenith model computers. With each of the above computers, a systems bootable floppy is needed to complete the escape to DOS. Applications with Exit to DOS utility may be able to break out of the user's menu. The "SET COMSPEC=COMMAND.COM /C' statement was unable to stop OFFICEWRITER or PROCOMM Exit to DOS utility. The DAC resultant from the user's menu does not have the granularity necessary to determine object ownership. The System Administrator (SA) must protect sensitive files residing on the hard disk with LOCKIT's file protection mechanisms.

File Level Protection. LOCKIT's encryption/decryption and file attribute programs does offer protection from unauthorized disclosure or read. Residual data not linked to a file access or alternation from utility programs such as Norton Utilities. Norton Utilities can also scan the hard disk for lost data not encrypted.

Object Reuse. LOCKIT provides satisfactory Object Reuse on files and system RAM. LOCKIT will not perform Object Reuse on free space for hard or floppy disk.

Audit. The Audit mechanism will not record unauthorized accesses. User activity is only recorded when the user operates from within his/her menu. The invalid login report records the last 16 attempts. An invalid user can conceal their user name and password recorded in the last 16 invalid logon attempts with 16 new invalid attempts. Invalid logon attempts are not recorded during Lunch-Break. The audit file is subject to the write vulnerability.

RECOMMENDATIONS:

I&A. The computer's cabinet cover should be locked to prevent anyone from removing the LOCKIT board.

DAC. The SA should disable the boot floppy drive after installation. while this recommendation posses an inconvenience, it will prevent a user from breaking out of the boot procedure as in the case with the Zenith, UNISYS, and Wang computers.

ASSESSED PRODUCT: Mace Utilities Version 1990.1 (DESTROY FILE Program)

VENDOR: Fifth Generation Systems, Incorporated

VERSION: 1990.1 (Maintenance Release for Version 1990)

DATE: May 1991

FINAL NISE EAST ASSESSMENT REPORT: No report number assigned

PRODUCT DESCRIPTION:

Mace Utilities uses an option called DESTROY FILE to perform its overwrite. Fifth Generation Systems, the Mace developer, claims the DESTROY FILE utility will permanently erase a file, making its data unrecoverable. They also claim it overwrites the file's directory entry to remove the pointer to the data cluster where the file began. Mace documentation also states that without the F OPTION, sophisticated technology exists for reading what was written on a disk even after it has been overwritten six times. As documented, the F OPTION claims to use DoD Standard 5220.22-M guidelines for data erasure, repeated seven times. The table below summarizes DESTROY FILE's claimed capabilities.

DESTROY FILE **DOS PROMPT COMMAND > DESTROY [drive] [path] filespec [options]**	
Options	Description
A	Automatically destroys files without querying. In the default mode, the programs asks for verification before destroying each file that matches the file specifications.
D	Destroys matching files in subdirectories of the named directory, but not the entire drive.
E	Destroys all "erased" (deleted) files on the drive in question, by overwriting all unused space on the drive. It does not, however, overwrite deleted directory entries.
H	Destroys HIDDEN files that match the file specification.
R	Destroys READ ONLY files that match the file specification.
S	Destroys SYSTEM files that match the file specification. NOTE: The default does not overwrite SYSTEM, HIDDEN, and READ ONLY files, even if they match the file specification.
F	Destroys all data on the disk using DoD Standard 5220.22-M erasure parameters.

ASSESSMENT SUMMARY:

In addition to the claimed DoD Standard 5220.22-M, Industrial Security Manual for Safeguarding Classified Information, March 1989, the DESTROY FILE assessment also used as principal compliance metrics; the DoD Magnetic Remanence Security Guideline, 15 November 1985, and the NISE EAST Automated Information Systems Remanence Security Guidebook, 19 September 1990.

DESTROY FILE safeguard features, specifically Option F, for the Magnetic Remanence do not comply with DoD guidelines for either a disk clear or disk purge routine. Specifically, rather than using a certain bit pattern followed by the complement pattern repeated three times, DESTROY FILE uses an unpredictable overwrite character for each pass. Moreover, DESTROY FILE sometimes enters unexplained endless loops or exhibits other unpredictable behavior.

ASSESSED PRODUCT: MAILSAFE Public Key Encryption

VENDOR: Fischer International Systems Corporation

VERSION: 5.0

DATE: December 1988

FINAL USAF-PERC ASSESSMENT REPORT: 88-703 31 March 1989

PRODUCT DESCRIPTION:

MAILSAFE can sign or authenticate messages. For electronic communications, MAILSAFE provides the security equivalent of the handwritten signature and envelope. MAILSAFE gives the user the ability to prove that a specific person signed a file. In addition, any file sealed in a MAILSAFE envelope can only be opened and read by the intended recipient. When MAILSAFE processes computer files, it performs two essential functions: appends an RSA Data Security, Incorporated, (RSA) Digital Signature to a file and creates an RSA Digital Envelope. MAILSAFE does not perform any communications functions; it is designed to create secure files for transfer within an existing communications system. MAILSAFE's public key system provides a unique set of two keys: private and public. Thus, other people who possess a copy of a public key can send secure electronic mail and can authenticate messages others send them. MAILSAFE protects your private key with a secret password you choose during key generation. An RSA Digital Signature also ensures that the contents of the file are correct and complete. If the file is not received by MAILSAFE exactly as it was sent, the program will tell if the signature is invalid. To assure absolute security, MAILSAFE includes an additional safety feature called "certification." In large or insecure computer systems, it's possible for an unauthorized person to tamper with public keys. To prevent such intrusion and to ensure that the public keys you have are genuine, they are certified. Certifying a public key is like adding your signature to that key. Keys can be certified by yourself or a trusted individual, such as the network administrator. Once you have certified a key your communications are safe, even if your keys or your correspondent's keys have been tampered with.

ASSESSMENT SUMMARY:

Since MAILSAFE is considered to be a security subsystem rather than a complete trusted computer system, it was assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes Identification and Authentication (I&A).

MAILSAFE, when tested on the Zenith Data Systems Z-150, Z-200, Z-248, and the Z-184 Laptop Computer, does effectively implement these mechanisms.

ASSESSED PRODUCT: Menu Works Advanced and Menu Works Total Security

VERSION: 2.2

VENDOR: PC Dynamics, Incorporated

FINAL ASSESSMENT REPORT: 94-503 27 May 1994

PRODUCT DESCRIPTION:

Menu Works Advanced is a software package that provides security protection of sensitive data on a personal computer. Some of the features of the menu facility include improved menu editor, single-key access to programs, restricting access to DOS, complete disk manager, custom screen design, built-in script language, and user login support.

Menu Works Total Security is used when maximum security is required. It uses Menu Works Advanced LOG ON screen and full system protection facilities and sits in the background monitoring system activity. It configures the entire system for the logged on user. Menu Works Total Security adds keyboard lockout during boot process, auto log off, directory protection, execute-only file protection, password protected DOS access functions, and log of all system activity, including failed log-on attempts.

ASSESSMENT SUMMARY:

The Menu Works program was assessed under the Computer Security Subsystem evaluation program. Although this program was considered to be a security subsystem rather than a complete trusted computer system, it was assessed against the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The security feature tested were I&A, DAC, Object Reuse, and Audit. In addition, the Disk Wipe (overwrite) option of the Menu Works Advanced program was assessed against the overwrite procedures outlined in the Air Force Systems Security Instruction Remanence Security (AFSSI 5020), 15 April 1991.

Menu Works Advanced and Menu Wor ks Total Security performed as advertised and is fully functional with its stated design purposes.

RECOMMENDATIONS:

Recommend Menu Works Total Security be installed and the security features be invoked when using Menu Works Advanced.

Recommend that the System Administrator exercise extreme care in determining user access to DOS and to utility programs that allow the user to alter attributes assigned by the System Administrator.

Recommend purging of the Audit log at regular intervals. This will ensure the integrity of the Audit trail will be maintained.

ASSESSED PRODUCT: Modified Hard Disk Control Cable

VENDOR: United States Air Force (AFSPACE-COM/XPXB)

VERSION: N/A

FINAL USAF-PERC ASSESSMENT REPORT: 90-502 May 1990

PRODUCT DESCRIPTION:

The Disk Control Cable is a special cable with the write function disabled. This allows the hard drive to read program files but does not allow any files to be written to the hard drive. Operation of the computer will be as normal. When the user enters an application, all of the menus are available to the system. Saving a file must then occur on a removable floppy disk. The hard disk drive is unable to save data because no data will be written to the disk.

The system gives the user the impression that data was written to the hard disk drive. However, when the PC is turned off and restarted, the file(s) will not be available anywhere on the hard disk drive. When a user tries gw copy a file onto the hard disk drive, the system directory gives the user the impression that the file was copied. However, when the user tries to access the file, it will not be available.

ASSESSMENT SUMMARY:

Although the Disk Control Cable was considered to be a security subsystem, it did provide Mandatory Access Control (MAC) by prohibiting any data to be written to the hard disk drive. The MAC mechanism was assessed against the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985.

The Disk Control Cable, when configured as tested on the Zenith Data Systems Z-248 computer, does effectively implement MAC. The Product Assessment and Certification Center (PACC) found no way to circumvent the write disable modification to the hard disk drive. However, the PACC found that even though no files were written to the hard disk, the files could be copied to drive A. In addition, the default settings of word processing programs could not be altered, additional fonts in printer programs could not be created, and additional files for a management programs could not be created.

Hardware modification of the PC is required to implement mandatory access control. This modification could impact the

warranty on the hardware. Recommend coordination with servicing contracting office prior to implementation.

ASSESSED PRODUCT: NoFBoot and SumFBoot

VENDOR: A. Padgett Peterson

VERSION: Alpha v.50 (NoFBoot)

DATE: October 1991

FINAL NISE EAST ASSESSMENT REPORT: No report number assigned

PRODUCT DESCRIPTION:

NoFBoot is a simple Terminate Stay Resident (TSR) program written by A. Padgett Peterson and distributed as FREEWARE. The purpose of this product is to prevent an inadvertent warm boot from a floppy disk (Ctrl-Atl-Del). NoFBoot intercepts the warm boot request and checks for a floppy disk in Drive A. If a disk is present, the boot is aborted, an error message is returned and any currently running program continues undisturbed. Otherwise, the request is granted and the boot proceeds normally. In order to boot from a floppy with NoFBoot running, a cold start is required (reset button or cycle power). The program, only 600 bytes long, is user transparent and can run under versions of MS-DOS from 2.10 to 5.0.

SumFBoot provides the exact same functionality as NoFBoot, as well as the added enhancement of being able to boot from a floppy disk by pressing Ctrl-Alt-F. In this case, a disk MUST be present in Drive A for the boot request to be accepted. An error message is returned when the Drive is empty.

ASSESSMENT SUMMARY:

NoFBoot and SumFBoot both operate exactly as the Product Description states, intercepting all warm boot requests and taking the proper action with regard to the status of Drive A. They are user transparent, until a warm boot request is made, and they don't adversely affect a running program if the request is denied.

These programs do have limitations as to their control over certain boot requests. Any program that directly issues a BIOS call to the reboot function, or another running TSR program that traps the warm boot function will bypass the NoFBoot and SumFBoot functionality.

A few bugs have been encountered using NoFBoot. NoFBoot will often allow warm boot requests through, with a floppy in drive A, when a number of CTRL-ALT-DEL are entered in succession. If a warm boot request is made while a program is loading into memory, the system will frequently lock up. A Columbia PC

(model VP-1600), with dual 640k floppies, was found to occasionally lock-up on attempted floppy boots. This situation was cleared by pressing Ctrl-Alt. Using graphics mode, it was found that the warm boot request was handled properly, but the error message was not displayed when the boot was denied. It is assumed that these bugs are also present in SumFBoot.

ASSESSED PRODUCT: Norton Commander

VENDOR: Symantec Corp. (formerly Peter Norton Computing, Inc.)

VERSION: 2.0

FINAL USAF-PERC ASSESSMENT REPORT: 89-507 June 1989

PRODUCT DESCRIPTION:

The Norton Commander (NC) programs consist of four programs and five files. The first four listed below (NC.EXT thru 123VIEW.EXE) are found on the distribution disk. The last five (NC.EXT thru DIRINFO) are created by NC.

o NC.EXE. This is the NC main program.

o NCSMALL.EXE. This is an optional program that runs NC using less memory.

o DBVIEW.EXE. A program that NC uses to display the contents of dBASE II and III files.

o 123VIEW.EXE. This pr ogram displays the contents of Lotus 1-2-3 and Symphony files.

o NC.EXT.This file defines the application programs to be associated with certain file extensions. It allows you to "point and shoot" files thereby loading them into the correct application with a single keystroke or mouse action.

o NC.INI. A file containing setup and preferences information. This file is created when you save the setup options and resides in the same directory as NC.EXE.

o NC.MNU. One or more files (one per directory) e ach defining a user menu of batch files.

o TREEINFO.NCD. A file containing the directory structure of your disk (fixed or floppy). It is created by NC in the root directory of each disk.

o DIRINFO. It is a text file used to label the directory. There may be a DIRINFO file in each directory.

NC offers a host of new and expanded features that make it more powerful, faster, and easier to use. The result is a powerful DOS enhancement shell that combines the functions of a hard disk manager with all the features you need to support and enhance the DOS command line.

ASSESSMENT SUMMARY:

Since NC is not considered to be a security subsystem, it was not assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 29 December 1985.

NC was assessed on the ZENITH Date Systems Z-150, Z-200, Z-248, and the Z-184 laptop computer and was found to function properly as stated in the manual.

ASSESSED PRODUCT: Norton Utilities WIPEFILE and WIPEDISK Programs Ver. 4.01

VENDOR: Symantec Corp. (formerly Peter Norton Computing, Inc.)

VERSION: 4.01

DATE: January 1989

FINAL USAF-PERC ASSESSMENT REPORT: 88-511 31 March 1989

PRODUCT DESCRIPTION:

WIPEFILE and WIPEDISK are separate programs within the Norton Utilities Version 4.01/Advanced Edition which supplements the DOS operating system. The WIPEFILE program overwrites and deletes files. Each file that matches the filespec is overwritten, which protects data by completely removing it. The data from files that have been overwritten is thoroughly lost and cannot be recovered or unerased. The WIPEFILE program is able to find and overwrite hidden and system files. It also is able to overwrite read-only files. However, it always pauses for confirmation before overwriting any of these files. The WIPEDISK program overwrites every portion of the disk, (Boot, File Allocation Table (FAT), Directory, and data areas), replacing all existing information with zeros (or any other value specified). This wipes a disk clean and safeguards data that was recorded on the disk. To meet government requirements, WIPEDISK allows you to specify the number of times the data is overwritten, and the overwrite value used. The latest DoD specifications (DoD 5220.22-M) specify that the 0/1 pattern should be repeated three times, followed by a write of a random value, then a verification of the last write. The default value is three overwrites.

ASSESSMENT SUMMARY:

Since the WIPEFILE and WIPEDISK programs were considered to be a security subsystem rather than a complete trusted computer system, they were assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes object reuse. In addition, the WIPEFILE and WIPEDISK programs were assessed against the overwrite procedures outlined in the Department of Defense Magnetic Remanence Security Guideline, 15 November 1985.

The WIPEFILE and WIPEDISK programs, when tested on the Zenith Data Systems Z-150, Z-200, Z-248, and the Z-184 Laptop Computer, do effectively implement the object reuse mechanism.

The WIPEDISK program was also found to have the capability of overwriting the bad sectors that are on either floppy or hard disks (removable or nonremovable).

ASSESSED PRODUCT: Norton Utilities Advanced Edition Programs (WIPEFILE and WIPEDISK) Ver. 4.5

VENDOR: Symantec Corp. (formerly Peter Norton Computing, Inc.)

VERSION: 4.5

DATE: March through April 1989

FINAL USAF-PERC ASSESSMENT REPORT: 89-506 10 July 1989

PRODUCT DESCRIPTION:

The Norton Utilities Version 4.5/Advanced Edition Programs include major improvements and additions for data recovery and disk management. Many of the programs allow for improved user interface and easier navigation with the programs. The WIPEFILE and WIPEDISK programs now support the latest Department of Defense security specifications, DoD 5220.22-M 116b(2).

WIPEFILE and WIPEDISK are separate programs within the Norton Utilities Version 4.5/Advanced Edition which supplement the DOS operating system. The WIPEFILE program protects classified data by overwriting and deleting files. Each file that matches the filespec is overwritten, which protects data by completely removing it. The data from files that have been overwritten is thoroughly lost and cannot be recovered or unerased. The WIPEFILE program is able to find and overwrite hidden and system files. It is also able to overwrite read-only files. However, WIPEFILE will always pause for confirmation before overwriting any of these files. The WIPEDISK program protects classified data by overwriting every portion of the disk (Boot, File Allocation Table (FAT), Directory, and data areas) and replacing all existing information with zeros (or with whatever other value you specify via the /Vn switch). This wipes a disk clean and destroys any classified data (along with all the other data) that was recorded on the disk. To meet government requirements, WIPEDISK allows you to specify the number of times the data is overwritten, and the overwrite value used. The latest DoD specifications [DoD 5220.22-M 116b(2)] specify that the 0/1 pattern should be repeated three times, followed by a write of a random value, then a verification of the last write. The default value is three overwrites.

ASSESSMENT SUMMARY:

Since the WIPEFILE and WIPEDISK programs were considered to be a security subsystem rather than a complete trusted

computer system, they were assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes object reuse. In addition, the WIPEFILE and WIPEDISK programs were assessed against the overwrite procedures outlined in the Department of Defense Magnetic Remanence Security Guideline, 15 November 1985.

The WIPEFILE and WIPEDISK programs, when tested on the Zenith Data Systems Z-150, Z-200, Z-248, and the Z-184 Laptop Computer, do effectively implement the object reuse mechanism. The WIPEDISK program was also found to have the capability of overwriting the bad sectors that are on either floppy or hard disks (removable and nonremovable). All other programs included in Norton Utilities Version 4.5/Advanced Edition Programs were found to function properly as stated in the manual.

ASSESSED PRODUCT: Norton Utilities Advanced Edition WIPEFILE and WIPEDISK Programs on Combat Personnel Control System (CPCS) TEMPEST Z-248

VENDOR: Symantec Corp. (formerly Peter Norton Computing, Incorporated)

VERSION: 4.5

FINAL USAF-PERC ASSESSMENT REPORT: 89-518 17 May 1990

PRODUCT DESCRIPTION:

WIPEFILE and WIPEDISK are separate programs within the Norton Utilities Version 4.5/Advanced Edition which supplement the DOS operating system. The WIPEFILE program protects classified data by overwriting and deleting files. Each file that matches the filespec is overwritten, which protects data by completely removing it. The data from files that have been overwritten is thoroughly lost and cannot be recovered or unerased. The WIPEFILE program is able to find and overwrite hidden and system files. It is also able to overwrite read-only files. However, WIPEFILE will always pause for confirmation before overwriting any of these files. The WIPEDISK program protects classified data by overwriting every portion of the disk (Boot, File Allocation Table (FAT), Directory, and data areas) and replacing all existing information with zeros (or with whatever other value you specify via the /Vn switch). This wipes a disk clean and destroys any classified data (along with all the other data) that was recorded on the disk. To meet government requirements, WIPEDISK allows you to specify the number of times the data is overwritten, and the overwrite value used. The latest DoD specifications [DoD 5220.22-M 116b(2)] require that the 0/1 pattern should be repeated three times, followed by a write of a random value, then a verification of the last write. The default value is three overwrites.

ASSESSMENT SUMMARY:

Although the WIPEFILE Version 4.5 and WIPEDISK Version 4.5 programs were considered to be a security subsystem rather than a complete trusted computer system, they were assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes object reuse. In addition, the WIPEFILE and WIPEDISK programs were assessed against the overwrite procedures outlined in the Department of Defense Magnetic Remanence Security Guideline, 15 November 1985.

The WIPEFILE and WIPEDISK programs of the Norton Utilities Version 4.5/Advanced Edition, when tested on the Combat Personnel Control System (CPCS) TEMPEST Z-248 computer, did not completely overwrite some of the clusters marked as **BAD** on the 130 MB. However, the PACC found that the **BAD** clusters contained no data.

The WIPEFILE Version 4.5 and WIPEDISK Version 4.5 programs did effectively wipe and delete files and overwrite the 130 MB removable hard disk and the 5.25-inch floppy disks.

ASSESSED PRODUCT: Norton Utilities Advanced Edition WIPEFILE and WIPEDISK Programs on COMPAQ 386/25

VENDOR: Symantec Corp. (formerly Peter Norton Computing, Incorporated)

VERSION: 4.5

FINAL USAF-PERC ASSESSMENT REPORT: 90-501 10 May 1990

PRODUCT DESCRIPTION:

WIPEFILE and WIPEDISK are separate programs within the Norton Utilities Version 4.5/Advanced Edition which supplement the DOS operating system. The WIPEFILE program protects classified data by overwriting and deleting files. Each file that matches the filespec is overwritten, which protects data by completely removing it. The data from files that have been overwritten is thoroughly lost and cannot be recovered or unerased. The WIPEFILE program is able to find and overwrite hidden and system files. It is also able to overwrite read-only files. However, WIPEFILE will always pause for confirmation before overwriting any of these files. The WIPEDISK program protects classified data by overwriting every portion of the disk (Boot, File Allocation Table (FAT), Directory, and data areas) and replacing all existing information with zeros (or with whatever other value you specify via the /Vn switch). This wipes a disk clean and destroys any classified data (along with all the other data) that was recorded on the disk. To meet government requirements, WIPEDISK allows you to specify the number of times the data is overwritten, and the overwrite value used. The latest DoD specifications [DoD 5220.22-M 116b(2)] specify that the 0/1 pattern should be repeated three times, followed by a write of a random value, then a verification of the last write. The default value is three overwrites.

ASSESSMENT SUMMARY:

Although the WIPEFILE Version 4.5 and WIPEDISK Version 4.5 programs were considered to be a security subsystem rather than a complete trusted computer system, they were assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes object reuse. In addition, the WIPEFILE and WIPEDISK programs were assessed against the overwrite procedures outlined in the Department of Defense Magnetic Remanence Security Guideline, 15 November 1985.

The WIPEFILE and WIPEDISK programs of the Norton Utilities Version 4.5/Advanced Edition, when tested on the COMPAQ Model 386/25 computer, did effectively wipe and delete files and overwrite the 110 MB nonremovable hard disk and the 5.25-inch floppy disks.

ASSESSED PRODUCT: Norton Utilities Advanced Edition WIPEFILE and WIPEDISK Programs on Sperry 3070-02

VENDOR: Symantec Corp. (formerly Peter Norton Computing, Incorporated)

VERSION: 4.5

FINAL USAF-PERC ASSESSMENT REPORT: 90-509 17 May 1990

PRODUCT DESCRIPTION:

WIPEFILE and WIPEDISK are separate programs within the Norton Utilities Version 4.5/Advanced Edition which supplement the DOS operating system. The WIPEFILE program protects classified data by overwriting and deleting files. Each file that matches the filespec is overwritten, which protects data by completely removing it. The data from files that have been overwritten is thoroughly lost and cannot be recovered or unerased. The WIPEFILE program is able to find and overwrite hidden and system files. It is also able to overwrite read-only files. However, WIPEFILE will always pause for confirmation before overwriting any of these files. The WIPEDISK program protects classified data by overwriting every portion of the disk (Boot, File Allocation Table (FAT), Directory, and data areas) and replacing all existing information with zeros (or with whatever other value you specify via the /Vn switch). This wipes a disk clean and destroys any classified data (along with all the other data) that was recorded on the disk. To meet government requirements, WIPEDISK allows you to specify the number of times the data is overwritten, and the overwrite value used. The latest DoD specifications [DoD 5220.22-M 116b(2)] specify that the 0/1 pattern should be repeated three times, followed by a write of a random value, then a verification of the last write. The default value is three overwrites.

ASSESSMENT SUMMARY:

Although the WIPEFILE Version 4.5 and WIPEDISK Version 4.5 programs were considered to be a security subsystem rather than a complete trusted computer system, they were assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes object reuse. In addition, the WIPEFILE and WIPEDISK programs were assessed against the overwrite procedures outlined in the Department of Defense Magnetic Remanence Security Guideline, 15 November 1985.

The WIPEFILE and WIPEDISK programs of the Norton Utilities Version 4.5 Advanced Edition, when tested on the Sperry Model 3070-02 computer, did effectively wipe and delete files and overwrite the 10 MB nonremovable hard disk and the 5.25-inch floppy disks.

ASSESSED PRODUCT: Norton Utilities Advanced Edition WIPEFILE and WIPEDISK Programs on UNISYS Desktop III

VENDOR: Symantec Corp. (formerly Peter Norton Computing, Incorporated)

VERSION: 4.5

FINAL USAF-PERC ASSESSMENT REPORT: 91-500 2 April 1991

PRODUCT DESCRIPTION:

WIPEFILE and WIPEDISK are separate programs within the Norton Utilities Version 4.5/Advanced Edition which supplement the DOS operating system. The WIPEFILE program protects classified data by overwriting and deleting files. Each file that matches the filespec is overwritten, which protects data by completely removing it. The data from files that have been overwritten is thoroughly lost and cannot be recovered or unerased. The WIPEFILE program is able to find and overwrite hidden and system files. It is also able to overwrite read-only files. However, WIPEFILE will always pause for confirmation before overwriting any of these files. The WIPEDISK program protects classified data by overwriting every portion of the disk (Boot, File Allocation Table (FAT), Directory, and data areas) and replacing all existing information with zeros (or with whatever other value you specify via the /Vn switch). This wipes a disk clean and destroys any classified data (along with all the other data) that was recorded on the disk. To meet government requirements, WIPEDISK allows you to specify the number of times the data is overwritten, and the overwrite value used. The latest DoD specifications [DoD 5220.22-M 116b(2)] specify that the 0/1 pattern should be repeated three times, followed by a write of a random value, then a verification of the last write. The default value is three overwrites.

ASSESSMENT SUMMARY:

Although the WIPEFILE Version 4.5 and WIPEDISK Version 4.5 programs were considered to be a security subsystem rather than a complete trusted computer system, they were assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes object reuse. In addition, the WIPEFILE and WIPEDISK programs were assessed against the overwrite procedures outlined in the Department of Defense Magnetic Remanence Security Guideline, 15 November 1985.

The WIPEDISK program of the Norton Utilities Version 4.5/Advanced Edition did not completely overwrite some of the clusters marked as **BAD** on the computer configurations (DTIII Model 800/16 and 800/12C). However, the PACC found that the **BAD** clusters contained no data. The WIPEFILE and WIPEDISK Version 4.5 programs were found to function as stated.

ASSESSED PRODUCT: Norton Utilities Programs Ver. 5.0

VENDOR: Symantec Corp. (formerly Peter Norton Computing, Inc.)

VERSION: 5.0

FINAL USAF-PERC ASSESSMENT REPORT: 90-515 10 May 1990

PRODUCT DESCRIPTION:

The Norton Utilities Version 5.0 contains 20 new or improved utilities for data recovery, disk repair, disk performance enhancement, and data security, plus convenient tools to ease such varied tasks as changing directories, finding files, and reporting system hardware information. Disk Monitor, Diskreet, and WipeInfo are separate utilities within the Norton Utilities Version 5.0 that provide data security.

The Disk Monitor utility provides functions to prevent any program from writing on the disk without approval. System areas, files, or entire disks can be protected from any form of writing. This can prevent many forms of viruses from completing their functions. It also protects the user from accidently erasing or overlaying important files and from formatting floppy drives or hard disks. The Diskreet utility protects confidential files so that they cannot be accessed without proper authority. Files are protected by encryption (i.e., they are encrypted on the disk and cannot be decrypted without the proper password). The Wipeinfo utility protects deleted confidential data by totally removing any traces of it from the disk so that unauthorized persons cannot recover it.

ASSESSMENT SUMMARY:

Although the Disk Monitor, Diskreet, and WipeInfo programs were considered to be a security subsystem rather than a complete trusted computer system, they were assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The security features tested included I&A, DAC, Object Reuse, and Audit. In addition, the Diskreet and WipeInfo utilities were assessed against the overwrite procedures outlined in the Department of Defense Magnetic Remanence Security Guideline, 15 November 1985.

The following security methods and mechanisms were found to function as stated:

o Proprietary and DES encryption methods

- Identification and Authentication (I&A)
- Discretionary Access Control (DAC)
- Object Reuse
- Audit

However, the PACC found that the write protection provided by the Disk Monitor program could be circumvented. This occurred when the Shell to DOS option on the Quit menu of the Disk Editor utility was selected. Files could be copied from floppy drives to hard disks and NDisks (reserved logical drive) or hard disks and NDisks to floppy drives, files could be created from word processing programs, and sub-directories could be created on floppy drives, hard disks, and NDisks. In addition, floppy drives, hard disks, and NDisks could be formatted, the default settings of application programs could be altered, additional fonts in printer programs and additional files for management programs could be created.

Continue to use all other programs of the Norton Utilities Version 5.0 programs for data recovery, improving disk performance, security, and simplifying and enhancing tasks.

ASSESSED PRODUCT: Norton Utilities Version 5.0 (WIPEINFO Program)

VENDOR: Symantec Corp. (formerly Peter Norton Computing, Inc.)

VERSION: 5.0 (Upgrade files dated **12-11-90**)

DATE: May 1991

FINAL NISE EAST ASSESSMENT REPORT: No report number assigned

PRODUCT DESCRIPTION:

The Norton Utilities overwrite procedure is WIPEINFO. WIPEINFO claims to safeguard data by totally obliterating it from the disk. Also, the documentation claims, sophisticated hardware and software cannot recover the data once WIPEINFO completes its procedure. As an added safety feature, WIPEINFO has built-in safe guards to avoid accidental data loss by prompting the user to respond to a warning message before the overwrite takes place. The following tables identify specific WIPEINFO claimed features for the Government compliant mode.

NORTON UTILITIES GOVERNMENT FAST WIPEINFO OPTIONS

Option	Description
Entire Disk	Purges an entire disk. Eradicates the system areas, as well as the directory and file areas. This procedure eliminates residual data. Multiple drives may be selected. The drive must be formatted prior to reuse.
Specific Files	Purges individual selected files.
Unused Disk Areas (Free Space)	Purges any residual data in clusters marked as free (with a 0) in the File Allocation Table (FAT). Two basic area types are applicable: **(1)** Files that have been deleted, but have not yet been overwritten with other files. **(2)** Clusters which may not have been used since the disk's most recent format, but which may contain residual data from the drive's previous use.
A File's Slack Area	Purges slack file space without affecting other file data.

CAUTION

A user must use the default **three** times repetition or ensure the repetition parameter is **three**. Otherwise, WIPEINFO's purge will not comply with DoD standards.

ASSESSMENT SUMMARY:

WIPEINFO serves as a security subsystem to perform the Magnetic Remanence safeguard feature. Accordingly, DoD Standard 5220.22-M, Industrial Security Manual for

Safeguarding Classified Information, March 1989; the DoD Magnetic Remanence Security Guideline, 15 November 1985; and, the NISE EAST Automated Information Systems Remanence Security Guidebook, 19 September 1990, were used as functional compliance metrics.

As claimed in the documentation, Norton Utilities comply with DoD standards for purging or clearing data recorded on disk media. Its human interface is especially suited for the novice and the experienced user alike. The compan ion tables indicate the assessment results for several different conditions.

CAUTIONS AND PRECAUTIONS:

WIPEINFO must be used with caution under four conditions:

■ Physica l Sectors Allocated to a Fixed Disk Partition Table. WIPEINFO does not overwrite sectors associated with the Partition Table. Thus, several thousand storage locations may be unaffected by its clear or purge functions; typically, all sectors (e.g., as many as 17 sectors) allocated to cylinder 0, side 0 will not be overwritten.

■ Physical Sectors in Logically Partitioned Disks. WIPEINFO does not overwrite sectors AFTER the logical disk partition but BEFORE the end of the physical disk. Typically, several thousand storage locations may be unaffected by its clear or purge functions.

■ File Slack Overwrite. Unless the upgrade version with files dated **12-11-90** is used, the WIPEINFO option to clear File Slack for hidden or read-only files will also reset the hidden, system, and read-only file attributes. Some programs rely on these attributes for "copy protection" or other feature purposes.

■ Bad Sectors. WIPEINFO does not overwrite any sector marked as "bad."

TESTED CONFIGURATIONS		
Computer	Operating System	Fixed Disk
Zenith Z-148	Z-DOS 3.3	None
Zenith Z-150	MS-DOS 3.3 and 4.0	10 and 10 megabyte partitions 20 megabyte full disk 30 megabyte full disk
ZEOS SX-20	DR DOS 5.0 and MS-DOS 4.0	30 and 45 megabyte partitions 37 and 38 megabyte partitions 80 megabyte full disk

ZEOS SX-16	MS-DOS 4.0	65 megabyte full disk

ASSESSED PRODUCT: Norton Utilities WipeInfo and DECLASFY Ver. 5.0 and 6.0

VENDOR: Symantec C orporation

VERSION: Version 5.0 and Version 6.0

FINAL USAF-PERC ASSESSMENT REPORT: 92-505 1 June 1992

PRODUCT DESCRIPTION:

WipeInfo Versions 5.0 and 6.0. WipeInfo is a separate program within the Norton Utilities which supplements the DOS operating system. WipeInfo protects deleted confidential data by totally removing any traces of it from the disk so that unauthorized persons cannot recover it.

WipeInfo has been designed with a safeguard to avoid accidental data loss. For each different wipe operation, a response to a warning message is necessary before the wipe operation takes place.

WipeInfo replaces WIPEDISK and WIPEFILE from previous versions of the Norton Utilities, combining both function into one utility.

DECLASFY Version 6.0. DECLASFY Version 6.0 is a program to declassify hard disks on IBM and compatible PC's. The program is designed to meet DOD standards concerning declassification of hard disks. The DOD requirements are that when declassifying hard disks the following procedure is required: write the entire disk with 0s, then 1s, and then random characters or symbols. This procedure is repeated three times.

ASSESSMENT SUMMARY:

WipeInfo Version 5.0 and 6.0:

- The WipeInfo programs did not completely overwrite all BAD clusters.
- The WipeInfo programs were found to function as stated.

DECLASFY Version 6.0. The DECLASFY program **DID NOT** function properly as stated.

RECOMMENDATIONS:

WipeInfo Version 5.0 and 6.0:

- Recommend verification of the wiped data if error messag es occur while overwriting BAD clusters with the WipeInfo programs on the removable hard disk on the CPCS TEMPEST Z-248 Computer.

NOTE: Clearing the 5.25-inch floppy disk requires either degaussing it or overwriting all locations with any character. Purging the floppy disk requires that it be degaussed.

- Recommend that other means be used (i.e., degaussing) if the GAD clusters contain data that cannot be overwritten by the WipeInfo programs.

- Use the WipeInfo programs to wipe files, file slack, wipe unused data areas only, and wipe entire disks.

- Use only the following configuration and options when initializing and executing these programs:

Government Wipe Configuration:

- Load WipeInfo from the Main Menu.

- Select "Configure" option from the WipeFile Menu.

- Select "Government Wipe" option from the Configuration Menu.

- Enter "3" for the wiping count. this is the number of times the wiping option will be repeated.

- Enter a wiping value (i.e., "246"). this is the value for the random character for the final overwrite.

- Select "Save settings".

This configuration sets up the government standard wipe method using the character value of 246 (hex F6) for the last overwrite.

Wipe Files:

- Load WipeInfo from the Main Menu.

- Select "Files" option from the WipeFile Menu.

- Enter drive (i.e., C:*.*, etc.) as the filename.

- Select "Include Subdirectories".

- Select "Confirm each file".
- Select "Hidden files".
- Select "Read-only files".
- Select "Wipe Files" as the wip ing method.
- Select "Wipe" to wipe all files on the disk.

This option, and the government Wipe Configuration will wipe all the files (hidden, read-only, etc.), including subdirectories, on the selected drive, using the method with a character value of 246 (hex F6) for the last overwrite.

NOTE: The file Slack option of the WipeInfo programs should be executed before the Wipe file option to ensure all residual data from the files are completely wiped from the disks.

File Slack:

- Load WipeInfo from the Main Menu.
- Select "Files" option from the WipeFile Menu.
- Enter "C:*.*" as the filename.
- Select "Include subdirectories".
- Select "Confirm each file".
- Select "Hidden files".
- Select "Read-only files".
- Select "Wipe unused file slack only" as the wiping method.
- Select "Wipe" to wipe all the slack areas.
- Select "Auto" from the Wiping files menu.

This option, and the government Wipe Configuration will automatically wipe the file slack on all the files (hidden, read-only, etc.), including subdirectories, on the selected drives, using the method with a character value of 246 (hex F6) for the last overwrite.

Wipe Unused Disk Areas Only:

- Load WipeInfo from the Main Menu.
- Select "Drives" option from the Wipefile Menu.
- Select "C:", "D:", etc. from the Wipe Drives menu.
- Select "Wipe unused areas only" as the wiping method.
- Select "Wipe" to wipe all unused areas on the disk.

This option, and the Government wipe Configuration will wipe the unused data areas on the selected drives using the method with a character value of 246 (hex F6) for the last overwrite.

Wipe Entire Disk:

- Load WipeInfo from the Main Menu.
- Select "Drives" option from the Wipefile Menu.
- Select "C:", "D:", etc. from the Wipe Drives menu.
- Select "Wipe entire drive".
- Select "Wipe" to wipe the entire disk.

this option, and the government Wipe configuration will wipe the Boot Records, FAT's Root Directories, and data areas on the selected drives using the method with a character value of 246 (hex F6) for the last overwrite.

DECLASFY Version 6.0:

- **DO NOT** use the DECLASFY Version 6.0 program to overwrite the 130-MB removable hard disk partitioned at three 33-MD plus on 31-MB.
- **DO NOT** use the DECLASFY program to wipe and delete files on the 5.25-inch 360-KB floppy disk.

ASSESSED PRODUCT: Norton Utilities WipeInfo 7.0

VERSION: Version 7.0

VENDOR: Symantec Corporation

FINAL ASSESSMENT REPORT: 93-506 30 September 1993

PRODUCT DESCRIPTION:

WipeInfo Version 7.0 is a separate program within the Norton Utilities which supplements the DOS operating system. WipeInfo protects deleted confidential data by totally removing any traces of it from the disk so that unauthorized persons cannot recover it.

WipeInfo has been designed with a safeguard to avoid accidental data loss. For each different wipe operation, a response to a warning message is necessary before the wipe operation takes place.

WipeInfo replaces WIPEDISK and WIPEFILE from previous versions of the Norton Utilities, combining both functions into one utility.

ASSESSMENT SUMMARY:

The WipeInfo Version 7.0 program was assessed under the Computer Security Subsystem evaluation program. Although this program was considered to be security subsystem rather than a complete trusted computer system, it was assessed against the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The security feature tested was object reuse. In addition, this program was assessed against the overwrite procedures outlined in the Air Force Systems Security Instruction (AFSSI) 5020 Remanence Security, 15 April 1991.

The WipeInfo program, when tested on the computer configurations listed in para 5.1, performed as advertised and is fully functional with its stated design purposes.

ASSESSED PRODUCT: Norton Utilities WipeInfo 8.0

VERSION: 8.0

VENDOR: Symantec Corporation

FINAL ASSESSMENT REPORT: 94-701 22 Aug 1994

PRODUCT DESCRIPTION:

WipeInfo Version 8.0 is a separate program within the Norton Utilities(a suit of programs which supplement the DOS operating system). WipeInfo protects data by totally removing any traces of it from disk so that unauthorized persons cannot recover it.

WipeInfo has been designed with a safguard to avoid accidental data loss. Before WipeInfo begins operation, it prompts the user with a warning message The user must then respond to continue with the operation.

WipeInfo replaces WIPEDISK and WIPEFILE from previous versions of the Norton Utilities, combining both functions into one utility.

ASSESSMENT SUMMARY:

The WipeInfo Version 8.0 program was assessed under the Computer Security Subsystem evaluation program. Although this program was considered to be a security subsystem rather than a complete trusted computer system, it was assessed against the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The security feature tested was object reuse. In addition, this program was assessed against the overwrite procedures outlined in the Air Force Systems Security Instruction Remanence Security (AFSSI 5020),15 April 1991. The WipeInfo program performed as advertised and is fully functional with it stated design purposes.

RECOMMENDATIONS:

Recommend verification of the wiped data if error messages occurs while overwriting BAD clusters with the WipeInfo program. Recommend that other means be used (i.e., degaussing) if the BAD clusters contain data that cannot be overwritten by the WipeInfo programs. Use the WipeInfo programs to wipe files, file slack, wipe unused data areas only, and wipe entire disks. Use the government wipe configuration and enter a 3 for the wiping option will be repeated. The File Slack option of the WipeInfo programs should be executed before the Wipe File option to ensure all

residual data from the files are completely wiped from this disks.

ASSESSED PRODUCT: NoZFBoot

VENDOR: NISE EAST

VERSION: 1.0

DATE: January 1992

FINAL NISE EAST ASSESSMENT REPORT: No report number assigned

PRODUCT DESCRIPTION:

NoZFBoot is a small program written specifically for use on a Zenith 248 system with a hard drive. NoZFBoot sets the CMOS BIOS such that all system boots, warm (Ctrl-Alt-Del) or cold (Power cycle), must be performed by the hard disk. If no hard disk is present, or if the program is run on a system other than a Zenith 248, an error message is returned. The program can run under versions of MS-DOS from 2.0 and above.

ASSESSMENT SUMMARY:

NoZFBoot operates exactly as the Product Description states, forcing all boot requests to be performed by the hard disk. Error messages are properly returned for systems without hard disks and non-Zenith systems.

The only ways to subvert this program would be: if the user directly accesses the system Setup (Ctrl-Alt-Ins) and changes the configuration to accept a boot-up from the A: drive, or if a program is run that allows the user to alter the configuration.

ASSESSED PRODUCT: ODCSOPS Automation Security Format (FILLDISK) Z-184

VENDOR: United States Air Force

DATE: November through December 1988

FINAL USAF-PERC ASSESSMENT REPORT: 88-506 20 June 1989

PRODUCT DESCRIPTION:

The ODCSOPS Automation Security Format (FILLDISK) software package consists of one diskette with a total of six files on it. They are:

- FILLDISK.EXE
- BIG.FIL
- UNSTART.BAT
- START.BAT
- READ.ME
- READ1.ME

The batch file "START.BAT" creates a temporary subdirectory called "[CDSI]" on drive C, copies two files to this subdirectory and runs the program "FILLDISK." When this program is finished, there will be a total of three files left in the subdirectory: FILLDISK.EXE, HUGE.FIL, and BIG.FIL. This will completely fill the hard disk.

ASSESSMENT SUMMARY:

Since ODCSOPS Automation Security Format was considered to be a nonsecurity subsystem, it was not assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985.

The ODCSOPS Automation Security Format, when invoked on the Zenith Data Systems Z -184 Laptop Computer with a hard disk, filled the unused portion of the hard disk. This prevented the creation of new files or the copying of files from another drive. However, this disk protection can be circumvented by the deletion of files within the hard disk. This would make the creation of new or classified files possible.

Refer to the Product Assessment Report, Project 88-506, 20 June 1989, for the recommended installation procedures for the FILLDISK program.

ASSESSED PRODUCT: ODCSOPS Automation Security Format (FILLDISK) Z-248

VENDOR: United States Air Force

DATE: May 1989

FINAL USAF-PERC ASSESSMENT REPORT: 89-508 20 June 1989

PRODUCT DESCRIPTION:

The ODCSOPS Automa tion Security Format (FILLDISK) software package consists of one diskette with a total of six files on it. They are:

- o FILLDISK.EXE
- o BIG.FIL
- o UNSTART.BAT
- o START.BAT
- o READ.ME
- o READ1.ME

The batch file "START.BAT" creates a temporary subdirectory called "[CDSI]" on drive C and then copies two files to this subdirectory and then runs the program "FILLDISK." When this program is finished, there will be a total of three files left in the subdirectory: FILLDISK.EXE, HUGE.FIL, and BIG.FIL. This will completely fill the hard disk.

ASSESSMENT SUMMARY:

Since FILLDISK is not considered to be a security subsystem, it was not assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985.

FILLDISK, when invoked on the Zenith Data Systems Z-248 with a fixed hard disk, filled the unused portion of the hard disk. This prevented the creation of new files or the copying of files from another drive. However, this disk protection can be circumvented by the deletion of files within the hard disk. This would make the creation of new or classified files possible.

Refer to the Product Assessment Report, Project 89-508, 20 June 1989, for the recommended installation procedures for the FILLDISK program.

ASSESSED PRODUCT: ODCSOPS Automation Security Format (FILLDISK) on UNISYS Desktop III

VENDOR: United States Air Force

VERSION: N/A

FINAL USAF-PERC ASSESSMENT REPORT: 91-508 18 July 1991

PRODUCT DESCRIPTION:

The ODCSOPS Automation Security Format (FILLDISK) software package, when invoked, will completely fill the unused portion of a hard disk.

ASSESSMENT SUMMARY:

Although this program was considered to be a security subsystem rather than a complete trusted computer system, it did provide Resource Access Control (RAC) by prohibiting any data to be written to the hard disk. The product was assessed against the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985, and AFR 205-16, 28 April 1989.

FILLDISK, when invoked on the UNISYS Desktop III Personal Workstation/2 (PW/2) 800/16 and 800/20C computers with a fixed hard disk or removable Bernoulli cartridge disk, filled the unused portion of the disks as stated in the product documentation. This prevented the creation of new files or the copying of files from another drive. However, these disk protection mechanisms can be circumvented by the deletion of files within the hard disks. This would make the creation of new or classified files possible.

FILLDISK only works when using a drive designation of **DRIVE C:** with only one partition. It **WILL NOT** work when using another drive designation or partition.

ASSESSED PRODUCT: Overwrite Program to Declassify Floppy or Hard Disks (KILLDISK) Version 3.0 and 4.0

VENDOR: Pan Am World Services

VERSION: 3.0 and 4.0

DATE: June 1988 through March 1989

FINAL USAF-PERC ASSESSMENT REPORT: 88-502 17 November 1988, Amendment 31 March 1989

PRODUCT DESCRIPTION:

KILLDISK is a microcomputer software package which operates on the Zenith Data Systems Z-150, Z-200, Z-248, and the Z-184 Laptop Computer (with internal 20 MB hard disk) using MS-DOS Version 3.1 or earlier. The product provides the ability to erase all storage media on the above mentioned systems.

The user enters KILLD ISK, a space, and then the disk drive that is to be overwritten (A:, B:, or C:) (KILLDISK A:). A warning message is displayed, alerting the user that the data in the specified drive will be destroyed, and that "CONTROL C" can be depressed to abort the overwrite. The KILLDISK software then proceeds to overwrite the entire disk with binary "1s", then with binary "0s", and finally with ASCII "A" characters. This completely overwrites the magnetic media three times. The user is then prompted to enter a number [of sectors that are] to be printed out to ensure the overwrite procedure was successful. A minimum of three sectors selected by the user must be printed or an error message will be received. Once this is complete, the user enters a "CONTROL C" and the computer is returned to the operating system to terminate the program.

ASSESSMENT SUMMARY:

Since KILLDISK Versions 3.0 and 4.0 were considered to be security subsystems rather than complete trusted computer systems, they were assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this pawduct includes object reuse. In addition, KILLDISK Versions 3.0 and 4.0 were assessed against the overwrite procedures outlined in the Department of Defense Magnetic Remanence Security Guideline, 15 November 1985.

KILLDISK Version 3.0. It was noted that when testing a 10 MB removable hard disk with no bad sectors, sectors zero and one were not overwritten. No useful data was ever written to or extracted from these two sectors as they always contained only the MS-DOS initial boot files. After utilizing KILLDISK to overwrite an entire disk and only printing out one sector for verification, "CONTROL C" was depressed and the user was

immediately returned to MS-DOS. In accordance with the KILLDISK documentation, an error message should have been received informing the user that at least three sectors had to be printed out before they could exit KILLDISK.

KILLDISK Version 3.0 could only be used to effectively overwrite 5.25-inch floppy disks formatted at 320 KB or 360 KB, 3.5-inch microfloppy disks formatted at 720 KB and also a formatted 10 MB removable hard disk, all of which contained no bad sectors. If any disks are formatted as indicated above and they do contain bad sectors, they must be overwritten/destroyed by another means other than KILLDISK.

KILLDISK Version 4.0. KILLDISK Version 4.0 could be used to effectively overwrite 3.5-inch microfloppy disks (formatted at 720 KB), 5.25-inch floppy disks (formatted at 320 KB or 360 KB), 10 MB removable hard disks (used on Z-150 and Z-200) and 20 MB nonremovable hard disks (used on the Z-248 and Z-184), all of which contained no bad sectors. If any disks are formatted as indicated above and they do contain bad sectors, they must be overwritten/ destroyed by another means other than KILLDISK.

In addition, KILLDISK Version 4.0 will overwrite sectors zero and one on the 10 MB removable hard disk and all sectors on the 20 MB nonremovable hard disks.

ASSESSED PRODUCT: Overwrite Program to Declassify Floppy or Hard Disks (KILLDISK) Version 5.0

VENDOR: Pan Am World Services

VERSION: 5.0

DATE: December 1989

FINAL USAF-PERC ASSESSMENT REPORT: 88-502 17 November 1988, Amendment 31 March 1989, 88-502A 18 December 1989

PRODUCT DESCRIPTION:

KILLDISK is a microcomputer software package which operates on the Zenith Data System Z-150, Z-200, Z-248, Z-386, and the Z-184 Laptop Computer (with internal 20 MB hard disk) using MS-DOS version 3.2 or earlier. The product provides the ability to erase all storage media on the above mentioned systems with the exception of the 53 MB hard disk on the Z-386.

The user enters KILLDISK, a space, and then the disk drive that is to be overwritten (A:, B:, C:, or D:) (KILLDISK C:). A warning message is displayed, alerting the user that the data on the specified drive will be destroyed, and that "CONTROL C" can be depressed to abort the overwrite. The KILLDISK software then proceeds to overwrite the entire disk with binary "1s", then with binary "0s" (three complete overwrites of each), and finally with the ASCII "A" characters. The user is then prompted to enter a number that is to be printed out to ensure the overwrite procedure was successful. A minimum of three sectors selected by the user must be printed or an error message will be received. Once this is complete, the user enters a "CONTROL C" and the computer is returned to the operating system to terminate the program.

ASSESSMENT SUMMARY:

Since KILLDISK was considered to be a security subsystem rather than a complete trusted computer system, it was assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes object reuse. In addition, KILLDISK was assessed against the overwrite procedures outlined in the Department of Defense Magnetic Remanence Security Guideline, 15 November 1985. Do not use KILLDISK on the Z-386 to overwrite 53 MB removable hard disks (partitioned at 32 MB and 20 MB).

KILLDISK can be used to overwrite 3.5-inch microfloppy disks (formatted at 720 KB), 5.25-inch floppy disks (formatted at 320 KB or 360 KB), 10 MB removable hard disks (used on the Z-

150, Z-200 and Z-386), and 20 MB nonremovable hard disks (used on the Z-258 and Z-184), all of which can contain bad sectors.

ASSESSED PRODUCT: Overwrite Program to Declassify Floppy or Hard Disks (KILLDISK) on Combat Personnel Control System TEMPEST Z-248

VENDOR: United States Air Force (AFCSC/SRMC)

VERSION: 5.0

FINAL USAF-PERC ASSESSMENT REPORT: 89-518 17 May 1990

PRODUCT DESCRIPTION:

KILLDISK Version 5.0 is a microcomputer software package which operates on the Zenith Data System Z-150, Z-200, Z-248, Z-386, and the Z-184 Laptop Computer using MS-DOS version 3.2.

The product provides the ability to erase all storage media on the above mentioned systems with the exception of the 53 MB hard disk on the Z-386.

The user enters KILLDISK, a space, and then the disk drive that is to be overwritten (A:, B:, C:, or D:) (KILLDISK A:). A warning message is displayed, alerting the user that the data on the specified drive will be destroyed, and that "CONTROL C" can be depressed to abort the overwrite. The KILLDISK Version 5.0 software then proceeds to overwrite the entire disk with binary one, then with binary zero, and finally with the ASCII "A" characters. This completely overwrites the magnetic media three times. The user is then prompted to enter a number that is to be printed out to ensure the overwrite procedure was successful. A minimum of three sectors selected by the user must be printed or an error message will be received. Once this is complete, the user enters a "CONTROL C" and the computer is returned to the operating system to terminate the program.

ASSESSMENT SUMMARY:

Do not use KILLDISK Version 5.0 to overwrite 130 MB removable hard disks partitioned at 33 MB, 33 MB, 31 MB and at 20 MB, 20 MB, 20 MB, and 20 MB on the CPCS TEMPEST Z-248 computer.

KILLDISK Version 5.0 did function properly on the 5.25-inch 360 KB floppy disk.

ASSESSED PRODUCT: Overwrite Program to Declassify Floppy or Hard Disks (KILLDISK) on COMPAQ 386/25

VENDOR: United States Air Force (AFCSC/SRMC)

VERSION: 5.0

FINAL USAF-PERC ASSESSMENT REPORT: 90-501 10 May 1990

PRODUCT DESCRIPTION:

KILLDISK Version 5.0 is a microcomputer software package which does not operate properly on the COMPAQ 386/25 using MS-DOS version 3.2.

The user enters KILLDISK, a space, and then the disk drive that is to be overwritten (A:, B:, C:, or D:) (KILLDISK A:). A warning message is displayed, alerting the user that the data on the specified drive will be destroyed, and that "CONTROL C" can be depressed to abort the overwrite. The KILLDISK Version 5.0 software then proceeds to overwrite the entire disk with binary one, then with binary zero, and finally with the ASCII "A" characters. This completely overwrites the magnetic media three times.

The user is then prompted to enter a number that is to be printed out to ensure the overwrite procedure was successful. A minimum of three sectors selected by the user must be printed or an error message will be received. Once this is complete, the user enters a "CONTROL C" and the computer is returned to the operating system to terminate the program.

ASSESSMENT SUMMARY:

Do not use KILLDISK Version 5.0 to overwrite 110 MB nonremovable hard disks (partitioned 20 MB, 75 MB, and 15 MB) on the COMPAQ Model 386/25 computer. In addition, do not use KILLDISK Version 5.0 to overwrite the 5.25-inch 1.2 MB floppy disk.

KILLDISK Version 5.0 did function properly on the 5.25-inch 360 KB floppy disk.

ASSESSED PRODUCT: Overwrite Program to Declassify Floppy or Hard Disks (KILLDISK) on Sperry 3070-02

VENDOR: United States Air Force (AFCSC/SRMC)

VERSION: 5.0

FINAL USAF-PERC ASSESSMENT REPORT: 90-509 17 May 1990

PRODUCT DESCRIPTION:

KILLDISK Version 5.0 is a microcomputer software package which does not operate properly on the Sperry 3070-02 using MS-DOS 3.2.

The user enters KILLDISK, a space, and then the disk drive that is to be overwritten (A:, B:, C:, or D:) (KILLDISK C:). A warning message is displayed, alerting the user that the data on the specified drive will be destroyed, and that "CONTROL C" can be depressed to abort the overwrite. The KILLDISK Version 5.0 software then proceeds to overwrite the entire disk with binary one, then with binary zero, and finally with the ASCII "A" characters. This completely overwrites the magnetic media three times. The user is then prompted to enter a number that is to be printed out to ensure the overwrite procedure was successful. A minimum of three sectors selected by the user must be printed or an error message will be received. Once this is complete, the user enters a "CONTROL C" and the computer is returned to the operating system to terminate the program.

ASSESSMENT SUMMARY:

Do not use KILLDISK Version 5.0 to overwrite 10 MB nonremovable hard disks on the Sperry Model 3070-02 computer.

KILLDISK Version 5.0 did function properly on the 5.25-inch 360 KB floppy disk.

ASSESSED PRODUCT: Overwrite Program to Declassify Floppy or Hard Disks (KILLDISK) on UNISYS Desktop III

VENDOR: United States Air Force (AFCSC/SRMC)

VERSION: 5.0

FINAL USAF-PERC ASSESSMENT REPORT: 91-507 5 August 1991

PRODUCT DESCRIPTION:

KILLDISK Version 5.0 is a microcomputer software package which does not operate properly on the UNISYS Desktop III using MS-DOS version 3.2.

The user enters KILLDISK, a space, and then the disk drive that is to be overwritten (A:, B:, C:, or D:) (KILLDISK C:). A warning message is displayed, alerting the user that the data on the specified drive will be destroyed, and that "CONTROL C" can be depressed to abort the overwrite. The KILLDISK Version 5.0 software then proceeds to overwrite the entire disk with binary one, then with binary zero, and finally with the ASCII "A" characters. This completely overwrites the magnetic media three times. The user is then prompted to enter a number that is to be printed out to ensure the overwrite procedure was successful. A minimum of three sectors selected by the user must be printed or an error message will be received. Once this is complete, the user enters a "CONTROL C" and the computer is returned to the operating system to terminate the program.

ASSESSMENT SUMMARY:

The security relevant characteristics of the product were compared against the claims of the vendor. Although this program was considered to be a security subsystem rather than a complete trusted computer system, it was assessed against the requirements for object reuse in the Department of Defense Magnetic Remanence Security Guideline (MRSG), 15 November 1985, and Air Force Systems Security Instruction (AFSSI) 5020 Remanence Security, 15 April 1991.

KILLDISK Version 5.0 **DID NOT** overwrite any sectors on the 320 MB nonremovable hard disks or the 42 MB removable Bernoulli cartridge disk on the UNISYS Desktop III Personal Workstation/2 (PW/2) 800/16 and 800/20C computers. It **DID NOT** completely overwrite the 3.5-inch 1.44 MB floppy drives.

KILLDISK Version 5.0 did function properly on the 5.25-inch 360 KB floppy.

DO NOT use KILLDISK Version 5.0 to overwrite the 320 MB nonremovable hard disks, the 42 MB Bernoulli cartridge disks, or the 3.5-inch 1.44 MB floppy drives.

Use the KILLDISK Version 5.0 program to clear 5.25-inch 360 KB floppy drives. **However, it is highly recommended that the floppy drives be purged according to instructions contained in AFSSI-5020.**

ASSESSED PRODUCT: PC/DACS

VENDOR: Pyramid Development Corporation

VERSION: 2.0

FINAL USAF-PERC ASSESSMENT REPORT: 89-501 16 April 1990

PRODUCT DESCRIPTION:

PC/DACS is a software package that is intended to control access to both the personal computer that it is installed on and the resources used in the PC. PC/DACS allows the design and construction of a security package which matches the needs of your environment. DACS ensures that security remains intact when the PC is booted by providing a Boot Protection mechanism option. This is done by placing the mechanism between the user and the system when the PC is booted. Users must enter a valid user ID and password combination before they are given access to the PC. Both the control Break and control "C" key combinations are disabled to prevent anyone from branching around DAC's log-on process. These key combinations are re-enabled after a successful log-on. Boot protection operates completely independently from the rest of PC/DACS. Other security functions provided by PC/DACS are Identification and Authentication (I&A), Discretionary Access Control (DAC), Object Reuse, and Audit. These mechanisms are essentially transparent to the user unless the user attempts to exceed his defined privileges.

ASSESSMENT SUMMARY:

Although the DACS programs were considered to be a security subsystem rather than a complete trusted computer system, they were assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The security features included I&A, DAC, Object Reuse, and Audit. In addition, the DACS Purge access rights program was assessed against the overwrite procedures outlined in the Department of Defense Magnetic Remanence Security Guideline, 15 November 1985.

DACS, when configured as tested on the Zenith Data Systems Z-150, Z-200, Z-248, Z-386, and the Z-184 laptop computers, does effectively implement the Boot Protection, I&A, DAC, and Object Reuse mechanisms. The Audit mechanism was found to provide an audit trail of PC activity. Although the mechanism could not be bypassed, the data in the files could be altered. In addition, the PACC found that once the audit data storage area (i.e., the disk) was exhausted, the PC could no longer perform auditable actions. When the system administrator (SA) attempted to produce an audit report, the system gave an error message and the PC locked up. The SA had to reboot the system and reset the audit file for the audit mechanism to function properly.

ASSESSED PRODUCT: PCSecure

VENDOR: United Sates Air Force (11 AF/SC)

VERSION: 1.0

FINAL USAF-PERC ASSESSMENT REPORT: 90-517 17 June 1990

PRODUCT DESCRIPTION:

The distribution disk, labeled PCSecure V1.0, 1 Oct 90, Master Copy, contained the following files:

- o PCSECURE.EXE
- o PCSECURE.C
- o PCSECURE.DOC

PCSecure is a security program that is completely command line driven. This feature allows the end users to set needed parameters in a batch file. The command line syntax is neither case nor order sensitive. The following examples are all in uppercase and shows the suggested order of the command line:

- o PCSECURE [drive...drives] [lock or unlock] [noprompt]
- o Example: PCSECURE C:LOCK NOPROMPT

The program name is PCSECURE. The next optional parameter is the drive or drives that need to be protected. In the example, drive C: is being locked. However, if there are other drives or logical drives, the command line could be changed to secure all drives.

The NOPROMPT option tells the command line NOT to ask the user if the drive is to be locked or unlocked. Without this optional command, a banner page explaining the function of the program is displayed and asks the user if it is to continue with the process of locking or unlocking.

PCSecure requires a work area on the disk that is to be secured. The exact size depends on the size of disk and number of files. For each 20 megabytes PCSecure will require 49K bytes plus 100 bytes for each file. PCSecure was developed using MS-DOS version 3.2 (Zenith) and MS-DOS 4.01. PCSecure **WILL NOT** secure drives larger than 40 MB.

ASSESSMENT SUMMARY:

The PCSecure program provided Resource Access Control (RAC) by prohibiting any data to be written to the hard disk for some configurations. The program was assessed against a subset of the requirements for mandatory access control (MAC) in the Department of Defense Trusted Computer System

Evaluation Criteria (TCSEC), 26 December 1985 and AFR 205-16, 28 April 1989.

PCSecure **DID NOT** secure the hard disks on the following test configurations:

- Zenith Z-248 with 20 MB and 40 MB Nonremovable Hard Disks
- Zenith Z-248 40 MB Nonremovable Hard Disk
- IBM PS/2 Model 50
- IBM PS/2 Model 70
- COMPAQ Deskpro 386/25
- UNISYS Desktop III PW/2 800/16
- UNISYS Desktop III PW/2 800/20C with 42 MB Removable Bernoulli Cartridge Disk
- UNISYS Desktop III PW/2 800/ 20C with 320 MB Nonremovable Hard Disk

PCSecure secured the hard disks on the following test configurations:

- Zenith Z-150
- Zenith Z-200
- Zenith Z-386
- Zenith Z-184
- IBM PS/2 Model 30
- Wang PC-280/20
- Wang PC-382
- COMPAQ SLT 286

ASSESSED PRODUCT: PC Tools Deluxe Version 6 (CLEAR FILE Option)

VENDOR: Central Point Software, Incorporated

VERSION: 6.0

DATE: May 1991

FINAL NISE EAST ASSESSMENT REPORT: No report number assigned

PRODUCT DESCRIPTION:

PC Tools Deluxe, distributed by Central Point Software, overwrite procedure is CLEAR FILE. The documentation claims CLEAR FILE will delete selected file(s) and then write a user definable bit pattern on the disk where file data was previously recorded. Central Point Software claims that the function will remove all data from the file(s) in a manner that cannot be UNDELETED. Specific claims for the CLEAR FILE function follow:

PC TOOLS DELUXE CLEAR FILE OPTIONS	
Option	Description
Default (Non-Government)	Overwrites one file using one cycle. The replacement hexadecimal value is F6 (the same character used by the DOS Format command to initialize a disk), or it can be user selected.
Government Standard	Overwrites different byte patterns, multiple times to a file(s). Replacement hexadecimal value is F6. **NOTE**: The documentation **DOES NOT** claim which government directive applies.

ASSESSMENT SUMMARY:

CLEAR FILE serves as a security subsystem to perform the Magnetic Remanence safeguard feature. Accordingly, DoD Standard 5220.22-M, Industrial Security Manual for Safeguarding Classified Information, March 1989; the DoD Magnetic Remanence Security Guideline, 15 November 1985; and, the NISE EAST Automated Information Systems Remanence Security Guidebook, 19 September 1990, were used as functional compliance metrics.

PC Tools Deluxe, Version 6, properly cleared disk files as claimed. However, it lacks a compliant disk purge capability stemming from its use of an ordered sequence of 01, 02, and so on, rather than those cited in DoD guidelines. The distinction between CLEAR and PURGE is an important consideration. A CLEAR routine should write at least one

known pattern to all storage areas. A PURGE routine should comply with DoD guidelines by writing a certain pattern followed by the pattern's complement, for three cycles. This action is followed by a known pattern's final overwrite and verification.

Operationally, the complete disk clear process is tedious since each directory must be selected and processed individually. The companion table indicates the assessment results for several different conditions.

PC TOOLS DELUXE VERSION 6.0
(Zenith Z-150 Computer)

Test Script Number	Summary Test Description	DOS Version	Critical Issue Compliance		
			Vendor	Purge	Clear
1	Sequentially Overwrite three (3) files, with each file nested within a separate sub-directory, within a 3-Tier directory tree structure, with a single command.	3.3 4.0	No Feature No Feature	-- --	-- --
2	Perform a Complete Floppy Disk A Overwrite.	3.3 4.0	See Note See Note	No No	Yes Yes
3	Perform a Complete Hard Disk C Overwrite.	3.3 4.0	See Note See Note	No No	Yes Yes
4	Overwrite One (1) File's Unused File Slack located in the Root Directory on a Hard Drive C.	3.3 4.0	No Feature	-- --	-- --
5	Overwrite One (1) File's Unused File Slack located in a 1-Tier directory tree structure on Hard Drive C.	3.3 4.0	No Feature No Feature	-- --	-- --
6	Overwrite One (1) File's Unused File Slack located in a 2-Tier directory tree structure on Hard Drive C.	3.3 4.0	No Feature No Feature	-- --	-- --
7	Overwrite One (1) File's Unused File Slack located in a 3-Tier directory tree structure on Hard Drive C.	3.3 4.0	No Feature No Feature	-- --	-- --
8	Sequentially Overwrite Three (3) File's Unused File Slack located in a 3-Tier directory tree structure on Hard Drive C.	3.3 4.0	No Feature No Feature	-- --	-- --
9	Perform a Complete Floppy Disk A Unused File Slack Overwrite.	3.3 4.0	No Feature No Feature	-- --	-- --
10	Perform a Complete Hard Disk C Unused File Slack Overwrite.	3.3 4.0	No Feature No Feature	-- --	-- --

Note: Each directory, or subdirectory, must be manually selected for clearing or purging.

ASSESSED PRODUCT: PC Tools Version 7 (WIPE Program)

VENDOR: Central Point Software

VERSION: 7

DATE: August 1991

FINAL NISE EAST ASSESSMENT REPORT: No report number assigned

PRODUCT DESCRIPTION:

The PC Tools Version 7, distributed by Central Point Software, overwrite procedure is WIPE. WIPE claims to safeguard data by totally obliterating it from the disk. Also, the documentation claims, that even sophisticated electronic means cannot recover the data once WIPE completes its procedure. As an added safety feature, WIPE has built-in safeguards to avoid accidental data loss by prompting the user to respond to a warning message before the overwrite takes place. The following table identifies the specific WIPE claimed features for the Government compliant mode.

PC TOOLS VERSION 7 GOVERNMENT WIPE OPTIONS

Option	Description
Entire Disk	Purges an entire disk. Eradicates the system areas, as well as the directory and file areas. This procedure eliminates residual data. The drive must be formatted prior to reuse.
Specific File(s) or Directory(ies)	Purges individually selected file(s) or directory(ies).
Unused Disk Areas (Free Space)	Purges any residual data in clusters marked as free (with a 0) in the File Allocation Table (FAT). Two basic unused disk area types are applicable: **(1)** Files that have been deleted, but have not yet been overwritten with other files. **(2)** Clusters which may not have been used since the disk's most recent format.
A File's Slack Area	Purges slack file space without affecting other file data.

CAUTION

You must use the default **three** times repetition or ensure the repetition parameter is **three**. Otherwise, the purge will not comply with DoD standards.

ASSESSMENT SUMMARY:

WIPE serves as a security subsystem to perform the Magnetic Remanence safeguard feature. Accordingly, DoD Standard 5220.22-M, Industrial Security Manual for Safeguarding Classified Information, March 1989; the DoD Magnetic Remanence Security Guideline, 15 November 1985; and, the NISE EAST Automated Information Systems Remanence Security Guidebook, 19 September 1990, were used as functional compliance metrics.

As claimed in the documentation, PC Tools Version 7 complies with DoD standards for purging or clearing data recorded on disk media. Its human interface provides easy-to-use pull-down menus, dialogue boxes, option lists, and on-screen advisories.

CAUTIONS AND PRECAUTIONS:

WIPE must be used with caution under three conditions:

- Physical Sectors Allocated to a Fixed Disk Partition Table. WIPE does not overwrite sectors associated with the Partition Table. Thus, several thousand storage locations may be unaffected by its clear or purge functions typically, all sectors (e.g., as many as 17 sectors) allocated to cylinder 0, side 0 will not be overwritten.

- Physical Sectors in Logically Partitioned Disks. WIPE does not overwrite sectors AFTER the logical disk partition but BEFORE the end of the physical disk. Typically, several thousand storage locations may be unaffected by its clear or purge functions.

- Bad Sectors. WIPE does not overwrite any sector marked as "bad."

TESTED CONFIGURATIONS		
Computer	Operating System	Fixed Disk
Zenith 150	MS-DOS 5.0	20 megabyte full disk
Zenith 150	MS-DOS 5.0	10 megabyte partition 2 megabyte partition
Zenith 150	Z-DOS 3.3	20 megabyte full disk
Zenith 150	Z-DOS 3.3	10.2 megabyte partition 1.02 megabyte partition 1.02 megabyte partition 1.02 megabyte partition
Zenith 248 AT	MS-DOS 5.0	Physical Disks: 20 megabyte Drive C 20 megabyte Drive D
ZEOS 386 SX	MS-DOS 5.0	65 megabyte full disk

ASSESSED PRODUCT: PC Tools Deluxe

VERSION: 7.1

VENDOR: Central Point Software Incorporated

FINAL ASSESSMENT REPORT: 92-501 10 December 1992

PRODUCT DESCRIPTION:

PC Tools Deluxe Version 7.1 (PC Tools 7.1). Central Point Software's PCTools 7.1 is a suite of programs designed to supplement the MS-DOS operating system. It provides the following features:

DOS Shell/File Manager (PC Shell). PC Tools' Shell Program is a utility program that includes all the critical DOS maintenance commands in a window environment. It provides the user with quick access to program and data files through a menuing system. You can use PC Shell to copy, move, delete, and compare files; edit files and disks; manage directories; and format disks. You can view database, spreadsheet, word processing, and graphics files in their native formats. PC Shell can be run as a terminate-and-stay-resident (TSR) program or as a stand-alone application.

Desktop Manager. Desktop Manager is PC Tools' desktop organizer. It can be set to run as a TAR or a standard DOS application. Features provided by Desktop Manager include a text editor, outliner, appointment scheduler, macroeditor, telecommunications capability, electronic mail, and database programs.

Hard Disk Backup. Central Point Backup (CP Backup) is an extensive program that backs up and restores user hard disk data. It supports multiple drive backups, unattended backups, high speed data compression, tape drives,variable user levels, and virus detection.

Commute. CP Commute is a comm unications software program. It provides the capability to run another computer by remote control.

Windows Utilities. PC Tools 7.1 Windows Utilities include a program launcher, scheduler, TAR manager, an undelete program, and the hard disk backup program. Many, but not all, of the other PC Tools utilities may also be run from a Windows 3.0 (or later).

Data Recovery and System Utilities. PC Tools 7.1 provides data recovery,data protection and security, performance, and system information. Data recovery features include undelete, disk or file fix, unformat, and recovery disk. Data

protection and security/features include mirror, data monitor,wipe, file and directory encryption, and virus detection. System utilities features include file compression, file find, and disk caching capabilities.

ASSESSMENT SUMMARY:

The PC Tools 7.1 DOS Shell/File Manager, Desktop Manager, Hard Disk Backup,Commute, Windows Utilities, and Data Recovery and System Utilities programs were assessed for their functionality, and were found to perform in accordance with the claims of the vendor.

The PC Tools 7.1 Wipe Program was assessed under the Computer Security Subsystem evaluation program. Although this program was considered to be a security subsystem rather than a complete trusted computer system, they were assessed against the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The security feature tested was object reuse. In addition, these programs were assessed against the overwrite procedures outlined in the Air Force Systems Security Instruction(AFSSI) 5020 Remanence Security, 15 April 1991.

The Wipe Program effectively purged all DOS addressable (data area)locations of the hard disk and floppy disks on the test bed systems. The file allocation table (FAT) and Root Directory Areas were cleared, while the Boot Record was left intact.

ASSESSED PRODUCT: Personal Computer Security System

VENDOR: Media Security Incorporated

DATE: Unknown

FINAL USAF-PERC ASSESSMENT REPORT: 87-501 9 December 1988

PRODUCT DESCRIPTION:

The Personal Computer Security System attempts noncooperative control by a combination of hardware devices that attempt to manage access to magnetic media. The product attempts to control physical access to removable magnetic media and read/write privileges to the media. It consists of a Perimeter Protection Unit (PPU), a Drive-Loc (DL), and an Electronic-Loc (EL).

The PPUs detect the entry and exit of personnel and will go into an alarm state if a diskette, specially coded by the EL, passes through them. A special disk drive, DL, allows only the specially coded diskettes to have data written to them. DL will not write to standard diskettes. The EL is a hardware addition to DL that protects information through an electronic coding process. It reads and writes to the media in a specially controlled format. This format provides a degree of privacy in that data cannot be retrieved without specialized analysis of the diskette. It is not encryption but a proprietary means of writing to the diskette.

ASSESSMENT SUMMARY:

Since the Personal Computer Security System is considered to be a security subsystem rather than a complete trusted computer system, it was assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes Security Design Criteria. Additionally, the Personal Computer Security System was assessed against the requirements of AFR 205-1, AFR 205-16 (1 August 1984), and the draft AFR 205-16 (August 1987) for Security Design Criteria. The product was also assessed for Functional Design Criteria.

The Personal Computer Security System does provide positive control by detecting the removal of controlled information. The product will help prevent low-level attempts at unauthorized disclosure and modification of information. However, the Personal Computer Security System does not meet the security design principles of the TCSEC, AFR 205-1, AFR 205-16, and draft AFR 205-16.

ASSESSED PRODUCT: PRIAM Hard Disk Formatting Software Programs

VENDOR: PRIAM Systems Division

VERSION: 4.02

FINAL USAF-PERC ASSESSMENT REPORT: 90-514 10 December 1990

PRODUCT DESCRIPTION:

The PRIAM Hard Disk Formatting Software programs perform the following four important functions:

- o defect list display
- o low- level drive formatting
- o surface analysis
- o configuration record maintenance

The defect list display allows the user to display on the screen the defect map and other data stored in the configuration records of the drive.

The low-level drive formatting is the process of writing the identification fields that are used to locate the sectors (data areas) on the drive. Formatting also flags defective sectors (those indicated in the configuration record) so that the operating system can avoid writing or reading to/from them. Finally, formatting establishes the sector interleave factor for the drive.

The interleave factor defines the order and location of sectors on the drive and has a dramatic effect on the performance of the drive. PRIAM drives are formatted at the factory with the optimum interleave factor for the CPCS TEMPEST Z-248 computer and controller used.

Surface analysis is the process of writing and reading the surface of the drive to locate sectors with possible media defects. It is performed at the factory using highly sensitive analog test equipment. A list of defects is shown on the label on top of the drive and written in the drive's configuration record. The list on the drive is updated by the surface analysis option of the EFMT.EXE program if new defects are found.

ASSESSMENT SUMMARY:

When configuration record maintenance is performed automatically each time the EFMT.EXE program is run it displays a message. Some utility programs may damage the configuration record.

Although the PRIAM Hard Disk Formatting Software programs were considered to be a security subsystem rather than a complete trusted computer system, they were assessed against the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The security features included object reuse in the Department of Defense Magnetic Remanence Security Guideline (MRSG), 15 November 1985.

The PRIAM Hard Disk Formatting Software programs, when invoked on the CPCS TEMPEST Z-248 computer, were found to function properly as stated. However, they **DID NOT** completely overwrite all **BAD** sectors that were listed in the Defect List Table.

Because the PRIAM Hard Disk Formatting Software programs do not meet the requirements of the Department of Defense Magnetic Remanence Security Guideline (MRSG), the programs should be used to overwrite unclassified information only.

ASSESSED PRODUCT: RAMPART-PC Menu System

VENDOR: Breakpoint Software, Inc.

VERSION: 3.03

FINAL USAF-PERC ASSESSMENT REPORT: 91-505 19 November 1991

PRODUCT DESCRIPTION:

RAMPART is a software based Discretionary Access Control facility for use on the IBM family of personal computers and 100% compatible machines.

ASSESSMENT SUMMARY:

The following are considered to be major problems because RAMPART **DOES NOT** provide adequate protection on the tested configurations:

- Hard Disk Lock and AES Boot Protection
- Identification and Authentication
- discretionary Access Con trol
- Audit
- AES encryption method

The following were found to function as stated in the vendors's documentation. However, they **DO NOT** provide adequate protection.

- RAMCRYPT and RAMDES encryption methods
- Object Reuse

RECOMMENDATIONS:

Recommend the system administrator (SA) disable the floppy disk drive so that the system cannot boot off any drive except the hard disk. This means that the A: drive on most systems and all floppy disk drives on Zenith systems (because of the Monitor program) will have to be physically disconnected after RAMPART is initially installed.

Recommend that the SA, when installing RAMPART, exercise extreme care in determining user access to utility programs such as Norton Utilities, PCTools, and MACE. These programs allow the user to alter attributes and resources assigned by the SA.

Recommend that this product not be used by the SA if a fully functional audit trail is required because of the strong possibility of invalid audit trail data being produced by the audit mechanism.

The Binary File Delete option of this product would be more functional if it included the following features:

- Completely remove the filename, size, and location from the directory.
- An option for overwriting to the unused or erased portions of a disk.

ASSESSED PRODUCT: Secure Electronic Bulletin Board System (SEBBS)

VENDOR: Naval Command, Control and Ocean Surveillance Center

In-Service Engineering East Coast Division

VERSION: 3

DATE: February 1991

FINAL NISE EAST ASSESSMENT REPORT: Secure Electronic Bulletin Board System (SEBBS), Zenith Z-248 Hosted Version, Technical Assessment Report, 28 February 1991

PRODUCT DESCRIPTION:

The Secure Electronic Bulletin Board System (SEBBS) melds a specially modified Remote Bulletin Board System - Personal Computer (RBBS-PC) software package, operating on a controlled and physically protected host computer, with the STU-III Access Control System (SACS) device. When operated in the Dedicated Security Mode, they provide secure electronic bulletin board services.

■ RBBS-PC. The SEBBS software, RBBS-PC, provides comprehensive electronic bulletin board services for message exchanges among its authorized correspondents, bulletins for review, and file upload and/or download services. It enforces mandatory access controls via a numerical security level privilege scheme. That is, the System Operator (SYSOP) grants each user a numerical privilege level associated with functions appropriate for that user. In turn, the SYSOP assigns all board functions a minimum privilege level necessary to access them (e.g., from essentially "all" users to none, not even the SYSOP personally). To access a certain function, the user's privilege level must be equal to or greater than the access level assigned to the requested function; otherwise, the attempted access will be denied. Other safeguards enforce discretionary access controls implemented by sub-privilege level and/or password protecting certain security critical functions (e.g., the ability to "download" a file from a specified directory). SEBBS safeguards also implement robust Identification and Authentication (I&A) features as well as protected, comprehensive security audit trail capabilities for all user activity, successful or not. The documentation suite includes a 200-page User's Manual detailing each option and giving suggestions for successfully installing and operating the system. In SEBBS service, other features include: an eight-line algorithm which records audit trail data from the STU-III; a Security Features User's Guide; and, a Trusted Facility Manual.

■ STU-III Access Control System (SACS). The Secure Telephone Unit (STU) III is a National Security Agency

approved device that provides secure voice and data capabilities. For SEBBS service, the AT&T STU-III's RS-232 data port feature provides the ability to use the STU-III as a protected auto-answer modem. In operation, the SACS feature gives cryptographically strong assurance that a calling STU-III's identity has been registered with the SEBBS' STU-III. It also ensures predetermined minimum and maximum security levels are consistent with the security policy for the particular SEBBS platform in question (e.g., UNCLASSIFIED, TOP SECRET). The SACS-equipped STU-III also provides ASCII data about the calling STU-III (e.g., its Keyset identity) and the mutually compatible session security level (e.g., SECRET) that can be processed by the SEBBS (e.g., for auditing caller accesses).

In short, the SEBBS software component, RBBS-PC, provides comprehensive electronic bulletin board service features, effective security safeguards, and full support for a System Security Officer (the SYSOP). Its complementary SACS-equipped STU-III provides cryptographically strong assurances that only specifically authorized users can gain access to SEBBS capabilities.

TESTED CONFIGURATIONS:

Highlights for the assessed configurations are as follows.

■ Hardware Configuration. The host computer was a Zenith Z-248 computer using a 20 megabyte hard disk for data storage. Secure connectivity at 2400 bps was provided by an AT&T STU-III Access Control System terminal directly connected to a dial telephone circuit. The calling party equipment was a Zenith 150 computer driving a Motorola STU-III, again directly connected to a dial telephone circuit. Additional SEBBS nodes for multiple user testing were made possible by using Alloy PC Slave/16N expansion boards. Slave activity was monitored using a Zenith micro computer configured as a terminal (fed by the PC Slave board's terminal port).

■ Operating System. Preliminary testing determined that neither the Zenith MS-DOS 3.2 nor their MS-DOS 3.3 would properly drive the PC Slave expansion board's networking software and the on-board disk drives. Due to this incompatibility, all tests used Microsoft MS-DOS 3.30 on the Z-248.

■ Software Configuration. RBBS-PC Version CPC17.3B, modified to add the functionality for recording STU-III audit information and recompiled into SEBBS.EXE, served as the software basis for all assessment scenarios. The NTNX/286 software driving the slaves was first configured to recognize only one slave, and after running tests in that configuration, reconfigured to recognize both slave boards. Procomm Plus

provided communica tions capability for the calling computers.

ASSESSMENT SUMMARY:

Even when subjected to malicious attacks designed to circumvent its security protection strategy and/or protected user-oriented features, SEBBS provided all claimed electronic bulletin board capabilities documented in its User's Manual effectively and efficiently.

- When configured properly and consistently with the security policy to be enforced for the specific SEBBS application and platform at hand, SEBBS security safeguards provide highly effective system-enforced protection against data compromise, data integrity loss, and service denial.

- Its chief strength lies in its cryptographically strong assurances that users reaching the main menu are in fact only those who have been explicitly registered with the system.

- Significantly, its I&A features assure its mandatory access controls and discretionary access controls uniquely enforce the system's security policy privileges for each user authorized to invoke explicitly protected electronic bulletin board capabilities or functions.

- Its protected audit trail gives complete information necessary to recreate events in detail should abuse or other improper activity be suspected.

Accordingly, when operated in the Dedicated Security Mode, SEBBS security safeguards protect sensitive unclassified and classified information entrusted to it at an acceptable risk level.

CAUTIONS AND PRECAUTIONS:

As with any complex, highly-valued system which provides important mission oriented services for its user community, SEBBS must be operated properly. The cautions and precautions listed below should be carefully observed.

- STU-III SACS. The STU-III Access Control System provides a superior method to control and limit access to SEBBS to only those users the SYSOP explicitly intends. Since the Keyset ID is a more precise calling terminal parameter than the DAO Code, the Keyset ID should be used to discriminate between authorized and unauthorized STU-IIIs.

- Doors. Using the RBBS-PC feature "Doors" (the ability to directly execute DOS commands and/or other applications programs remotely) could bypass the safeguards implemented in SEBBS. Accordingly, "doors" must be disabled for SEBBS security safeguard assurances to remain intact.

■ File Upload Authority. Consistent with its planned mission operational use, file upload authori ty should be explicitly limited to trusted subscribers.

■ File and Message Protection. Testing graphically illustrated that the SYSOP must both configure SEBBS and maintain accurate hard-copy password assignment records via sound configuration management procedures.

-- Both files and messages controls use security level parameters set in the CONFIG program for SEBBS. Those parameters have roughly 64,000 different security levels. Without hard-copy, accurate records, it is difficult to balance granting proper access with guarding against increased risks for undesira ble actions and increased SYSOP maintenance workload.

-- In addition to the security levels assigned to menu commands, the SYSOP can establish a separate files-security file, named FILESEC, to control access to files, groups of files, or even entire DOS subdirectories. That file can control access either by security level, by password, or both. The SYSOP must exercise care to adhere to FILESEC format requirements. Filenames, directo ries, security levels and passwords must conform to the prescribed security file structures, and must be entered exactly.

■ Conferences and Sub-Boards. Conference and Sub-Board testing uncovered an area needing careful attention.

-- A conference is a separate message area within SEBBS, primarily oriented toward users with common interests. Confer ences maintain separate message files, and may maintain separate users files. Security level require ments for features and functions within a conference are identical to those in the main board.

-- A sub-board is essentially a separate electronic bulletin board within the main board. The key difference between the two is that a sub-board may be uniquely configured in all areas except the communications parameters that allow the user to initially access the main board. Like a conference, the SYSOP may establish a minimum security level assignment needed to access the sub-board. However, the security levels needed to access all sub-board functions can be individually configured. This concept, if not implemented carefully, can allow a user access to features not otherwise authorized. [See also the SEBBS Trusted Facility Manual.]

■ Service Denial. Service quality can suffer should a suitably motivated user desire to monopolize the board indefinitely (or until the SYSOP intervenes). Users should be admonished to use care in this regard.

ASSESSED PRODUCT: Secure Copy Version 1.0

VENDOR: United States Air Force

VERSION: 1.0

DATE: July 1989

FINAL USAF-PERC ASSESSMENT REPORT: 89-511 30 August 1989

PRODUCT DESCRIPTION:

The Secure Copy software package consists of one diskette with a total of two files on it. They are:

- o SCOPY.EXE
- o SCOPY.C

The program SCOPY.EXE, written in "C" language, copies a file from either a floppy or hard disk to another floppy disk. It will overwrite the last buffer to remove any remanence after the last valid character. This program could be useful in creating an output floppy of a lesser classification than the classification level at which the system normally operates.

ASSESSMENT SUMMARY:

Since Secure Copy is not considered to be a security subsystem, it was not assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985.

The Secure Copy program, when invoked on the Zenith Data System Z-150, Z-200, Z-248, Z-386, and the Z-184 Laptop Computers, was found to function properly as stated. However, unpredictable results occurred when copying files of 60K bytes or larger to the diskettes.

ASSESSED PRODUCT: SECUREPC

VENDOR: Hughes Data Systems, Incorporated

VERSION: 3.31

DATE: June through July 1989

FINAL USAF-PERC ASSESSMENT REPORT: 89-510 30 August 1989

PRODUCT DESCRIPTION:

SECUREPC is a software package that provides security protection of sensitive data on a personal computer (PC). The front end security, the Hard Disk Bootup mechanism, prevents unauthorized access to the hard disk(s). SECUREPC protects the PC during the boot sequence and afterwards by intercepting all Control/C and Control/Break keystrokes. Control/C and Control/Break have no effect on SECUREPC. Once the PC has booted, access to the PC is given to those users who identify themselves with the proper identification code and its associated user password. Other security functions provided by SECUREPC are Identification and Authentication (I&A), Discretionary Access Control (DAC), object reuse, and audit. These mechanisms are essentially transparent to the user unless the user attempts to exceed his defined privileges.

ASSESSMENT SUMMARY:

Since SECUREPC was considered to be a security subsystem rather than a complete trusted computer system, it was assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes I&A, DAC, object reuse, and audit. In addition, the File Scrub program was accessed against the overwrite procedures outlined in the Department of Defense Magnetic Remanence Security Guideline, 15 November 1985.

SECUREPC, when configured as tested on the Zenith Data Systems Z-150, Z-200, Z-248, Z-386, and the Z-184 Laptop Computers, does effectively implement the Hard Disk Bootup, I&A, and object reuse. The DAC was found to function properly using access decision techniques at the DOS interface. However, the DAC user attributes could be altered using various disk utility programs. This allowed the user to access DAC facilities that were not originally authorized. The audit mechanism was found to provide an audit trail of PC activity. Although the audit mechanism could not be bypassed, the user Timelog files could be erased. In addition, the data in the Timelog files could be altered using various disk utility programs.

ASSESSED PRODUCT: SecurePC and SecurePC PLUS

VENDOR: Hughes Data Systems, Incorporated

VERSION: 5.0

FINAL USAF-PERC ASSESSMENT REPORT: 91-512 1 September 1993

PRODUCT DESCRIPTION:

SecurePC. SecurePC is a software package that provides security protection of sensitive data on a personal computer (PC). The front end security, a BOOTLOCK mechanism provided by SecurePC, prevents unauthorized access to hard disk(s). booting from the floppy disk and then attempting to access any hard disk returns the massage "Invalid Drive Specification." All hard disks, physical as well as logical, are protected by SecurePC.

Secure of the security functions provided by SecurePC are: Identification and Authentication (I&A), Discretionary Access Control (DAC), Object Reuse, and Audit.

SecurePC PLUS. SecurePC PLUS is used when maximum security is required. It uses SecurePC's LOG ON screen and full system protection facilities and sits in the background (Terminate and Stay Resident) and monitors system activity. It configures the entire system for the logged on user. SecurePC PLUS adds file level security and event auditing.

ASSESSMENT SUMMARY:

SecurePC. SecurePC and its options were found to function as stated in the vendors' documentation.

The Following security mechanisms were found to function as stated in the TCSEC and AFSSI 5020 documentation:

- Identification and Authentication
- Object Reuse

The following security mechanisms are considered to be problems because SecurePC does not provide adequate file protection on the test configurations according to the TCSEC documentation:

- DAC
- Audit

SecurePC PLUS. SecurePC PLUS and its options were found to function according to the vendors' documentation.

SecurePC PLUS and its DAC security mechanism was found to function according to the TCSEC documentation.

RECOMMENDATIONS:

Recommend SecurePC PLUS be **INVOKED** when using SecurePC. This will limit the access an unpriviledged user has when they temporarily leave a program, such as Windows, and try to perform a function using the DOS commands.

Recommend that the master administrator (MA), when installing SecurePC and SecurePC PLUS, exercise extreme care in determining user's access to DOS and the setting of the Time and Date from within the DOS Utility Menu. this would limit the strong possibility of invalid audit data being produced by the audit mechanism.

Recommend that the MA, when installing SecurePC and SecurePC PLUS, exercise extreme care in determining user access to DOS and to utility programs such as Norton Utilities, PCTools, etc. These programs allow the user to alter attributes and resources assigned by the MA>

Recommend that the MA, when invoking SecurePC PLUS, exercise care in limiting the number of files contained on the Bootup drive. This would prevent having Bootup problems with the PCs.

ASSESSED PRODUCT: TriSpan Workstation Manager (Trispan)

VENDOR: Micronyx Incorporated

VERSION: 1.033

DATE: March through April 1988

FINAL USAF-PERC ASSESSMENT REPORT: 88-504 17 November 1988

PRODUCT DESCRIPTION:

Trispan is an add-on security product that consists of an expansion board, personal identification tokens, and supporting software utilities. The expansion board itself provides user Identification and Authentication (I&A), Discretionary Access Control (DAC) on objects, DAC on system resources (RAC), object reuse, and audit mechanisms. The I&A mechanism is used in conjunction with a personal identification token. In addition to the security features listed above, Trispan uses an intricate memory management scheme, referred to as the Controlled Access Mechanism (CAM), to protect the resources on its expansion board. The CAM disallows random access to the information on the board by only allowing access through specific controlled entry points within the workstation's address space. The software utilities provide the ability to alter the specific characteristics of the security mechanism. In addition, a manager program is provided to access the Trispan configuration data such as user profiles and general system security parameters.

ASSESSMENT SUMMARY:

Since Trispan is considered to be a security subsystem rather than a complete trusted computer system, it was assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes I&A, DAC, object reuse, and audit.

Trispan, when configured as tested on the Zenith Data Systems Z-150 and Z-200, does effectively implement the DAC, object reuse, audit, and CAM mechanisms. However, the I&A mechanism could be bypassed using the Monitor ROM program; access was granted to any user prior to entering all requested I&A information. In addition, the MANAGER program, used to control the I&A mechanism, was found to be accessible by any user. By executing the MANAGER program, the user was able to alter the state of execution configuration of the Trispan board. The DAC was found to function properly using high-level access decision techniques at the DOS interface. In the low-level DAC, the DAC mechanism could be bypassed using disk utility programs. Although the DAC file descriptors could be circumvented, the data retrieved was in an encrypted form, other than "public" which is not encrypted.

ASSESSED PRODUCT: V-PHAGE

VENDOR: Application C onfiguration Computers, Inc.

VERSION: 2.1

FINAL USAF-PERC ASSESSMENT REPORT: 91-515 13 November 1991

PRODUCT DESCRIPTION:

V-PHAGE is software which monitors DOS to secure IBM and compatible computers or networks. V-PHAGE functions at the platform-level (e.g. computer) taking control of the operating system (O/S) upon cold boot (warm boots are locked out).

ASSESSMENT SUMMARY:

The following are considered to be major problems because V-PHAGE does not provide adequate protection of the tested configurations:

- Identification and Authentication
- Discretionary Access Control
- Audit

The following were found to function as stated in the documentation:

- V-PHAGE encryption methods
- Object Reuse

RECOMMENDATIONS:

Recommend disabling the floppy disk drive so that the system cannot boot off any drive except the hard disk. this probably means that the A: drive on most systems and all floppy disk drives on Zenith systems (because of the Monitor program) will have to be physically disconnected. This would prevent a user from altering and/or deleting various files using utility programs such as Norton Utilities, PCTools, and MACE.

The Product Assessment Certification Center (PACC) recommends that the system administrator (SA), when installing V=PHAGE, exercise extreme care in determining user access to utility programs such as Norton Utilities, PCTools, and MACE. These programs would allow the user to alter his/her accesses assigned by the SA.

Recommend that this product not be used by the SA if a fully functional audit trail is required because of the strong

possibility of invalid audit trail data being produced by the Audit mechanism.

The File Erase option would be more functional if it included the following features:

- Completely remove the filename, size and location from the directory
- An additional option for overwriting to the unused or erased portions of a disk

ASSESSED PRODUCT: Watchdog

VENDOR: Fischer International Systems Corporation

VERSION: 5.1

DATE: December 1988 through February 1989

FINAL USAF-PERC ASSESSMENT REPORT: 88-701 31 March 1989

PRODUCT DESCRIPTION:

Watchdog is a microcomputer software package comprised of three system diskettes: System Administrator Diskette, Program Diskette, and Audit Trail Diskette. It provides Identification and Authentication (I&A), Discretionary Access Control (DAC), object reuse, and audit. A Watchdog Armor card, which is optional, provides maximum protection of the data and programs stored on the personal computer.

Watchdog provides access control to programs and files while maintaining user separation, user log-on procedures, and elimination of previous user's data work space from memory. Watchdog also provides data protection by encrypting stored information. The Watchdog system provides for one System Administrator (SA). The SA is responsible for installing the Watchdog security features into the microcomputer to be protected. The SA generates, loads, and archives passwords and identifications. He designates which of the Watchdog users will have access to data areas. In this way, Watchdog protected microcomputers can be organized for the function of sharing information among multiple users. The SA is the only user who can alter his own profile.

ASSESSMENT SUMMARY:

Since Watchdog is considered to be a security subsystem rather than a complete trusted computer system, it was assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes I&A, DAC, object reuse, and audit.

Watchdog, when configured as tested on the Zenith Data Systems Z-150, Z-200, and Z-248 does effectively implement the object reuse and audit mechanisms. However, the I&A mechanism could be bypassed on the Z-150, Z-200, and Z-248. Access was granted to any user prior to entering all requested I&A information. Although access was granted, one could not run any of the executable programs, but could change directories and delete files within those directories.

In addition, the DAC mechanism could be bypassed on the Z-150 and Z-200 using disk utility programs. It was found that one

could read or write to any sector on the disk and file names were found in sector areas that were protected by encryption.

ASSESSED PRODUCT: Watchdog Armor

VENDOR: Fischer International Systems Corporation

VERSION: 1.0

DATE: December 1988 through February 1989

FINAL USAF-PERC ASSESSMENT REPORT: 88-702 31 March 1989

PRODUCT DESCRIPTION:

Watchdog Armor is an optional feature that works with Watchdog Version 5.1. It provides for security mechanisms that include: Protected Security Firmware, Hard Disk Boot Up, Hardware Data Encryption Standard (DES), and a Tamper-Proof System Clock that is used with the audit mechanism. These security mechanisms provide maximum protection of the data and programs stored on the personal computer. Watchdog Armor is comprised of an expansion board and supporting software utilities. The expansion board itself provides some of the security mechanisms. The software utilities provide the ability to install the card, set the Armor clock, initialize RAM, and run a diagnostic test on the card. The System Administrator (SA) is the individual responsible for installing Watchdog security features into the microcomputer which is to be protected.

ASSESSMENT SUMMARY:

Since Watchdog Armor is considered to be a security subsystem rather than a complete trusted computer system, it was assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes audit.

Watchdog Armor, when configured as tested on the Zenith Data Systems Z-150, Z-200, and Z-248 does effectively implement the Protected Security Firmware, Hardware Data Encryption Standard (DES), and the Tamper-Proof System Clock mechanisms. However, the Hard Disk Boot Up mechanism could be bypassed on the Z-150, Z-200, and Z-248. By using a diagnostic utility program on drive A, one could read/write to drive C on the Z-150 and Z-200. Access to drive C was denied on the Z-248.

THIS PAGE INTENTIONALLY BLANK

3.2 MACINTOSH SECURITY PRODUCTS

ASSESSED PRODUCT: MacTools Deluxe

VENDOR: Central Point Software

VERSION: Not Applicable

DATE: August 1991

FINAL NISE EAST ASSESSMENT REPORT: No report number assigned

PRODUCT DESCRIPTION:

Distributed by Central Point Software, MacTools Deluxe's overwrite procedure has been included in the Optimizer utility. MacTools Deluxe Optimizer Erase features safeguard data by totally erasing it from the disk. Central Point Software claims that "MacTools Deluxe has been designed to meet the Defense Investigative Service (DIS) erasure requirements for classified data." To avoid accidental data loss, it has a built-in safety feature that prompts the user to respond to a warning message before the overwrite actually takes place. The following tables identify specific Optimizer claimed features for the Government compliant overwrite mode.

MacTools Deluxe VENDOR CLAIMS FOR ERASING FILES, DIRECTORIES, DISKS or DISKETTES	
Options	Option Description
Erase Free Space	Writes over all the unused disk area, including previously deleted files, with either ones, zeros, or alternating ones or zeros. This process erases unused tracks and deleted files and guarantees that both the unused free space and space occupied by deleted files will be completely eradicated.
Erase Hard Disk Volumes	Writes over the entire disk, block by block, using ones, zeros, or alternating ones and zeros for a specified number of cycles. This process erases the directory blocks and creates a new directory. This procedure guarantees that all data on the disk is totally erased and unrecoverable.

ASSESSMENT SUMMARY:

Optimizer Erase utility serves as a Magn etic Remanence safeguard feature. Therefore, the DoD Magnetic Remanence Security Guideline, 15 November 1985, and the NISE EAST Automated Information Systems Remanence Security Guidebook, 19 September 1990, served as the assessment criteria.

Although the documentation claims it "... has been designed to meet Defense Investigative Service (DIS) erasure requirements for classified data.", MacTools Deluxe does not comply with DoD standards for either purging or clearing data recorded on disk media. Specifically, it fails to perform the "write, verify, and retain any last character" steps for purging, or, the "verify and retain any character" steps for clearing.

The companion tables indicate the assessment results for several different conditions.

TESTED CONFIGURATIONS		
Computer	Operating System	Disk Drives
Macintosh Plus	System Version 6.0.3 Finder Version 6.1	20 Megabyte Hard Disk 800 Kilobyte Internal Disk Drive 400 Kilobyte External Disk Drive

MacTools Deluxe ASSESSMENT TEST SYNOPSIS					
Test Script Number	Summary Test Description	Operating System	Critical Issue Compliance		
			Vendor	Purge	Clear
1	Perform an "erase free space" overwrite on an 800k diskette that included deleted files.	System 6.0.3 Finder 6.1	Yes	No	No
2	Perform an "erase free space" overwrite on a 20 megabyte hard disk that included deleted files.	System 6.0.3 Finder 6.1	Yes	No	No
3	Perform a complete 800K diskette overwrite.	System 6.0.3 Finder 6.1	Yes	No	No
4	Perform a complete 20 megabyte hard disk overwrite.	System 6.0.3 Finder 6.1	Yes	No	No

ASSESSED PRODUCT: Norton Utilities WipeInfo (Macintosh System) version 2.0

VENDOR: Symantec Corporation

FINAL ASSESSMENT REPORT: 94-501 24 June 1994

PRODUCT DESCRIPTION:

WipeInfo Version 2.0 is a separate program within the Norton Utilities (a suit of programs which supplement the Macintosh operating system). WipeInfor is designed to destroy previous written data by writing new, meaningless data over every addressable location on hard disks and diskettes. The program is self-protecting in that it cannot perform its destructive actions against the start-up system disk or the disk that contains its own active program.

ASSESSMENT SUMMARY:

The WipeInfo Version 2.0 program was assessed under the Computer Security Subsystem evaluation program. Although this program was considered to be a security subsystem rather than a complete trusted computer system, it was assessed against the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The security feature tested was object reuse. In addition, this program was assessed against the overwrite procedures outlined in the Air Force Systems Security Instruction Remanence Security (AFSSI 5020), 15 April 1991.

WipeInfo Version 2.0 for the Macintosh and all of its options were found to function properly as stated in the program documentation. The program will overwrite all addressable locations on external, internal, small computer system interface (SCSI) drives and partition disk with the Macintosh Hierarchial File System (HFS). However, it will not recognized non-Macintosh partition disks. WipeInfo does meet the minimum Dad standard for overwriting magnetic media. However, it does not meet the overwrite criteria outlined in AFSSI 5020. The program will only allow users to make either one or three overwrite passes. Moreover, it does not have a built-in option that will allow users to specify more than three overwrite passes.

RECOMMENDATIONS:

Recommend executing the Wipe Disk option three times, using the government wipe option. When a user encounters an error, recommend the user verify that there is no classified or readable data in that sector where the error occurred. Also, if any errors occur while overwriting, of if any unusable sector/track could not be overwritten, recommend using an approved degausser to purge the data from the hard disk.

ASSESSED PRODUCT: Symantec Utilities for MacIntosh

VENDOR: Symantec Corporation

VERSION: 2

FINAL USAF-PERC ASSESSMENT REPORT: 91-503 26 February 1992

PRODUCT DESCRIPTION:

Symantec Utilities for MacIntosh Version 2 (called SUM II hereafter) is a collection of utility programs that keeps MacIntosh disks operating at peak performance, protects them from disk problems, and provides an encryption scheme to protect data. SUM II gives the user the capability to recover data if he/she accidentally deletes a file from a disk, crashes a hard disk, or happens to initialize a hard disk for mistake. MacIntosh Version 4.2 and Finer Version 6.0 or higher is required.

The SUM Partition program lets the user divide a hard disk into separate volumes allowing the use of each volume (partition) as a separate hard disk. This program also lets the user protect individual partitions by encrypting the data and assigning a password to the partition. This program also works with floppy disks, allowing a user to encrypt and password protect data on the disk.

The SUM TuneUp program keeps a hard disk operating at peak performance by defragmenting files and optimizing the way space is used. This program also overwrites all unused areas on a disk and locks out all bad sectors.

ASSESSMENT SUMMARY:

The SUM Partition password protection program does require users to enter a valid password before gaining access to a password protected partition. However, the Identification mechanism was not designed into this program; therefore, users are not required to identify themselves before gaining access to a protected partition. Only a valid password is required. The Product Assessment and Certification Center (PACC) was unable to break the password protection mechanism; however, the encrypted partition attributes could be altered. This allowed access to the encrypted partition, but the data inside the encrypted partition remained encrypted and unreadable.

SUM TuneUp's Erase Free Space option purge d all unused data in the data area, with both the minimum or maximum number of repetitions. However, the boot block, used in the data areas were not overwritten. Also, if a user invokes the Lock Out Bad Sectors option first, the Erase Free Space option did not overwrite the bad sectors. The bad sectors are considered

as used areas and any area considered in use will not be overwritten. In addition, since the Verify file option only checked for read errors, a separate disk editing utility program is needed to verify that the data was removed out of the bad sectors. The Erase Free Space option alone should not be used to declassify disks.

NOTE: SUM II programs do not recognize nor overwrite non-MacIntosh partitions. Also, SUM TuneUp works only with Hierarchical File System (HFS) format. It does not work on volume partitions or diskettes less than 800K in size.

RECOMMENDATIONS:

Authentication. When typing the initial password for the first time in the SUM Partition program, users should be careful that no one is looking over their shoulder because the password is echoed on the screen. NOTE: The password is echoed on the screen when typing the initial password. After that an asterisk (*) symbol is echoed instead of the password.

Object Reuse:

Users should run the Erase Free Space option first before they run the Lock Out Bad Sector option. Also, after verifying that all sectors in the data area were overwritten (with a disk editing utility program), launch the SUM TuneUp again and run the Lock Out Bad Sectors. the Lock Out Bad Sectors option detects ad sectors and "flags" them so that data cannot be written into those sectors. A separate disk editing utility program should be used to verify that all data in the bad sectors were overwritten.

SUM TuneUp's Verify File Option verifies that each and every file on the volume can be rad properly. However, there is no option to allow a user to interrupt the overwrite cycle to verify that the correct pattern was written. A separate utility program is needed for this.

the SUM TuneUp's Erase Free Space option purged all unused data in the data area. However, the security could be enhanced if the program had an additional option to initialize the disk and overwrite all areas of the disk. This includes purging the boot block, volume information block, volume bit map, extents tree, and all areas marked as used in the data area.

ASSESSED PRODUCT: The Viper

VENDOR: Systematic Computer Services

VERSION: 1.0a3

DATE: 4 December 1990 through 15 January 1991

FINAL USAF-PERC ASSESSMENT REPORT: 90-510 14 December 1990

PRODUCT DESCRIPTION:

The Viper is a single function program designed to overwrite data on 800K and 1440K high density diskettes and Apple HFS compatible disks in Apple Macintosh Plus, SE, IIx, and IICx Computers. The Viper will not overwrite 400K diskettes. The program allows up to six cycles of overwrites using a bit pattern of alternating ones and zeros followed by a randomly generated cycle of overwrite data. The overwrite procedure consists of three distinct functions: the Zero function, which does clear the disk directory, but does **not** erase the data area assigned to the file structure; the Verify function, which simply reads each bit from the disk, but does not verify that the disk has been overwritten or zeroed; and, the Format function; which is the destructive portion of the program and also makes use of both the Zero and Verify functions. The program is self-protecting in that it cannot perform its destructive actions against the logged system disk or the disk that contains its own active program.

The Viper generates a report of its action which includes: original disk information, user options selected, last backup date, date of overwrite, and elapsed time. This requires a printer to be either directly connected or attached via a network, as long as it is Quickdraw compatible and Chooser selectable. The Viper can also generate reports on an Imagewriter or Laserwriter, or by using image drivers such as LinkSaver.

The Viper does not take advantage of Multifinder features; therefore, Macintosh System File version 6.02 and Finder version 6.1 or later are needed.

ASSESSMENT SUMMARY:

Since The Viper is considered to be a security subsystem rather than a complete trusted computer system, it was assessed against a subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The subset for this product includes object reuse. In addition, The Viper was assessed against the overwrite procedures outlined in the Department of Defense Automated Data Processing Security Manual (DoD 5200.28-M), January 1973 and AFR 205-16, April 1989.

Tests were performed by executing The Viper program on 800K and 1440K high density diskettes, as well as an internal hard disk, on the Macintosh IIx, IICx, and SE. Each of the Viper options: Zero, Verify, and Format were tested, as well as the number of repetitions (2-6) of overwrites. No data was found on any disks after the rewrite procedure (Format function) was executed, whether with the minimum number of repetitions or the maximum. The Viper Version 1.0a3 was found to function properly as described in the documentation. Its performance was sufficient to meet the criteria of the National Policy and Air Force Regulation.

RECOMMENDATION:

Since the Format function of The Viper automatically calls the Zero function, the Zero option should be removed. The Zero function chosen alone may give a false sense of security to a user who believes that they are zeroing the disk, when in reality they are only zeroing the directory and leaving the data untouched.

It is important to point out that The Viper's functions: Zero, Verify, and Format are **not** what their names imply. The user should therefore be familiar with how these functions operate in order to avoid inadvertent erasure of data or failure to properly overwrite the intended data.

ASSESSED PRODUCT: VIPER

VERSION: 1.01

VENDOR: Systematic Computer Services

FINAL ASSESSMENT REPORT: 91-501 15 May 1991

PRODUCT DESCRIPTION:

The Viper Version 1.01 is a single function program designed to overwrite data on 800K and 1440K high density diskettes, and Apple HFS (Hierarchical File System) compatible disks [both Small Computer Systems Interface (SCSI)and non-SCSI] in Apple Macintosh Plus, SE, II, IICX, and IIX computers.Macintosh operating system Version 6.0.2 or higher and Finder Version 6.1 or higher is required. The Viper will not overwrite 400K diskettes. The program allows the user to choose from one to six cycles of overwrites using a user selectable bit pattern of alternating binary 1s and binary 0s. The complement of the user selected pattern is automatically calculated for the second write of that cycle. A write cycle finishes with a randomly generated pattern of overwrite data. The Viper then generates a report of its action which includes: original disk information, user options selected, last backup date, date of overwrite, elapsed time, number of overwrite errors, and number of verify errors. The program is self-protecting in that it cannot perform its destructive actions against the startup system disk or the disk that contains its own active program.

ASSESSMENT SUMMARY:

The Viper was tested on the following platforms Macintosh Plus, SE, II,IICX, and IIX computers. The overwrite algorithms for object reuse are consistent with national policy in form and function, as stated in the Department of Defense Automated Data Processing Security Manual (DoD 5200.28-M), Department of Defense Magnetic Remanence Security Guideline(MRSG) (15 Nov 85), Computer Security Policy, AFR 205-16 (28 April 89), and Remanence Security, AFSSI 5020 (15 April 91). The program performs as advertised and is fully functional with its stated design purposes within three constraints. First, if the program is interrupted during the overwrite cycle (e.g., a power failure), the target disk must be re-initialized before the Viper program c an be re-launched against the media to complete the overwrite function. Second, since The Viper is dependent on the disk driver that is currently installed on a system to tell it which blocks are writable,fixed disks should be cleared prior to updating disk drivers (e.g., when upgrading to a higher operating system version). This will avoid the problem of blocks being marked as bad and inaccessible (and therefore unable to be cleared

with The Viper) by the new driver that were considered good by the old driver. Finally, The Viper program does not recognize nor over written on Macintosh partitions (e.g., A/UX). When operated heeding these three precautions, the Viper Version 1.01 does perform to the levels of the national policy for clearing magnetic media. However, since the Viper Verify function provides only a check for read errors, a separate utility program (e.g., Norton Utilities or MacTools) is needed to verify that the data has been removed in such a manner that the media may be declassified by security personnel authorized to do so.

THIS PAGE INTENTIONALLY BLANK

3.3 SYSTEMS SECURITY PRODUCTS

ASSESSED PRODUCT: PC-Disk (AT&T 3B2/600G)

VENDOR: AT&T

VERSION: 2.0

FINAL USAF-PERC ASSESSMENT REPORT: 92-503A 5 May 1992

PRODUCT DESCRIPTION:

The PC-Disk Release 2.0 utility is used to read, write, and format a floppy disk residing on an AT&T 3B2/600G computer. Files (text or binary) can be copied from an MS-DOS floppy disk to a 3B2 host and vice versa. the floppy disk can be formatted in a 320K format (8 sectors per track) or a 360K format (9 sectors per track). PC-Disk Release 2.0 was installed on an AT&T 3B2/600G minicomputer running UNIX System V Release 3.2.3 with system V/MLS Release 1.2.1.

ASSESSMENT SUMMARY:

PC-Disk Release 2.0 does not violate the System V/MLS Release 1.2.1 security policy. an object reuse problem was noted during the assessment which could result in a "need-to-know" violation; however, this risk can be minimized by operational procedures. It was discovered that if a large file is copied to the diskette before a small file is written, within the same PC-Disk session, residual data (filling up the remainder of a logical block of 1024-byte block) from the large file is appended to the small file. Also, a potential denial-of-service condition could exist if a user does not relinquish exclusive use of the diskette drive after completing a transfer session.

RECOMMENDATIONS:

To minimize the risk from the object reuse problem noted in above, all diskettes written to during a PC-Disk session should only be released to individuals that have the need-to-know for **all** of the information written to diskettes during the PC-Disk session. Another alternative is to exit the PC-Disk application before inserting a new diskette into the drive.

The system administrator should periodically issue the request(1S) command without any arguments to ensure that the diskette drive is not unnecessarily tied up by a user that unintentionally, or intentionally, did not release access. The request command, without arguments, will display the current status of all requestable devices. If the device is shown as "in use" and the requesting user is not using it (which can be determined by ps -ef | grep pcdisk), the system administrator should release the device.

The physical security of the 3B2 cabinet is an integral part of the overall system security. the root password can be circumvented and changed if an individual is allowed physical access to the cabinet and console for about 20 minutes. Therefore, each site should determine if ordinary users should have physical access to the 3B2 cabinet. It follows that if users are not allowed physical access to the disk drive, the use of PC-Disk by users will require system administrator intervention to inset and remove diskettes. If you only want the system administrator to run PC-Disk, use chmod(1S) to remove execute permission for others on PC-Disk (chmod 554 /usr/bin/pcdisk). If the decision is made to disallow users from

executing pcdisk, we recommend that execute permission also be disabled for request(1S) and release(1S). this will eliminate the denial-of-service condition previously discussed.

ASSESSED PRODUCT: Sanitization Software for the AT&T 3B2/600G

VENDOR: AT&T

VERSION: 1.1.0

FINAL USAF-PERC ASSESSMENT REPORT: 91-506 13 August 1991

PRODUCT DESCRIPTION:

The Sanitization Software product can be ordered as Sub Line Item Number (SLIN) 0012AH off the Standard Multiuser Small Computer Contract (SMSCRC). It was developed specifically to meet the SMSCRC requirements and runs on the AT&T 3B2/600G. The product provides three utilities that provide a means to overwrite "main" memory, removable and non-removable magnetic hard disks, and magnetic tape.

ASSESSMENT SUMMARY:

A software utility is provided for overwriting all areas of the removable and non-removable disk storage. In addition, the utility provides a means for viewing and printing operator-selected and random portions of the overwritten disk media for verification. Although the utility functions as advertised by the vendor, it does not meet the overwriting procedures for **purging** magnetic hard disks that is specified in AFSSI-5020, Remanence Security, 15 April 1991. AFSSI-5020 states that to **purge** a magnetic hard disk, an "overwrite cycle consists of writing a character (such as binary 0) to every addressable location, then writing its complement (binary 1) to every addressable location. After at least three overwrite cycles, write a single alphanumeric character to all locations." The Sanitization Software performs a simple media format operation that only writes a pattern to every addressable location once. The utility is sufficient, however, to **clear** magnetic hard disks.

Another utility is provided to overwrite "main" memory. The utility sets each addressable memory location alternatively to binary 1s and binary 0s until the state is changed either 100 or 1000 times as specified by the user. The utility functioned as advertised; however, since main memory on the 3B2/600G is volatile Random Access Memory (RAM), it cannot be **purged** by overwriting. Paragraph 6-1.b. of AFSSI-5020 states that volatile semiconductor memory is to be purged by "removing power (including backup power) for a minimum of 30 seconds."

The product also provides a utility to overwrite magnetic tapes. The over write pattern is written once and a means of viewing and printing portions of the overwritten tape is also provided. The utility functioned as advertised. Although this utility suffices to **clear** magnetic tapes, it does not meet the **purging** requirements in AFSSI-5020. The note under paragraph 4-1.b. of AFSSI-5020 states "Do not overwrite floppy disks or magnetic tapes or **purge** data. Degauss them."

Although the Sanitization Software functions as advertised, it does not satisfy the purging requirement to declassify magnetic hard disks or tapes as stated in AFSSI-5020. Three overwrite cycles of complementary binary patterns is required to purge memory on the 3B2/600G; users
should follow the guidance in AFSSI-5020 in lieu of using the main memory overwrite utility. AFSSI-5020 requires the removal of power from main memory (RAM) for purging.

THIS PAGE INTENTIONALLY BLANK

3.4 ANTI-VIRAL PRODUCTS

ASSESSED PRODUCT: Disinfectant

VENDOR: Freeware (Disinfectant is part of the Computer Security Toolkit. (Contact your local Information Systems Security Manager for a copy.)

VERSION: 2.5.1

FINAL USAF-PERC ASSESSMENT REPORT: 90-707 9 October 1991

PRODUCT DESCRIPTION:

Disinfectant will scan Apple Macintosh diskettes or stand alone systems and identify any existing Macintosh virus infections that can be detected using this product. It will inform the user which files or system areas are infected and will provide the ID (name) of the virus strain that has caused the infection. It will also repair files which have been infected by the viruses without harming the file.

Disinfectant recognizes the Scores, nVIR, INIT 29, ANTI, MacMag, WDEF, ZUC, MDEF, Frankie, and CDEF viruses. It also recognizes all the known variations and clones of these viruses. Furthermore, it also recognizes many possible unknown variations and clones. Disinfectant does not recognize the "Dukakis" virus, which only propagates between HyperCard stacks and is very rare.

Disinfectant also includes a virus protection startup document (INIT). When properly installed, the Disinfectant INIT will protect an uninfected system against infection by any of the known Mac viruses. If an infected application starts to run, the Disinfectant INIT will beep and inform the user that the application is infected with a virus. It will then prevent the infected application from executing.

Disinfectant has an extensive help menu and will pri nt out a user's manual over sixty pages in length.

ASSESSMENT SUMMARY:

Disinfectant was evaluated using a testbed of four viruses, Scores, nVIR A, nVIR B, and WDEF A which are the most prevalent viruses affecting Air Force Macintosh systems. These four viruses account for about 95% of the virus incidents reported to AFCSC/SR.

USER GUIDANCE:

Disinfectant should be executed from a bootable, write-protected floppy disk when scanning a hard drive on a system. Do not use Disinfectant to scan individual files or folders if running System 7. A new version, Disinfectant 3.0, is currently under development to correct this problem and take advantage of System 7 features such as balloon help.

NOTE:

This application is freeware. The author, John Norstad of Northwestern University, has granted permission for anyone to make and distribute copies of Disinfectant. It may not be sold or distributed for profit.

ASSESSED PRODUCT: F-PROT Professional Anti -Virus Software

VERSION: 2.07

VENDOR: COMMAND Software Systems, Incorporated

FINAL ASSESSMENT REPORT: 92-507 22 June 1993

PRODUCT DESCRIPTION:

F-PROT Professional is an antiviral software package that provides the capability to scan over 2000 known viruses and provides the following functionality:

Prevents infected programs from loading.

Scans for unknown viruses using a heuristic analysis method.

Scans for boot sector viruses.

Scans network disk drives.

Scans for Trojan Horse s.

Disinfects affected files.

Protects resident portion of the software from becoming infected via Stealth feature.

Maintains a file integrity database to further ensure the integrity of system and data files.

ASSESSMENT SUMMARY:

The F-PROT Professional software assessment was specifically directed toward the functionality of VIRSTOP.EXE, F-PROT.EXE (non-interactive and interactive mode), and CHECK.EXE programs. The purpose was to assess the software's installation procedure, how the user may configure it to perform virus scans on a personal computer, and to determine whether the software performed as advertised by the vendor.

F-PROT Professional's installation, configuration, file integrity checker, and virus scanning and their options were found to function as stated in the vendors' documentation. The F-PROT Professional assessment report can be found in Appendix A.

Once F-PROT Professional was installed in memory, it was able to prevent 128 viruses tested from infecting the test configuration. It is recommended that the file integrity

checker option be used in conjunction with the F -PROT Anti-Virus software. It provides added security protection to the system.

ASSESSED PRODUCT: VirHUNT

VENDOR: Digital Dispatch, Inc.

VERSION: N/A

FINAL USAF-PERC ASSESSMENT REPORT: 90-704A 14 April 1991

PRODUCT DESCRIPTION:

VirHUNT is a virus detection, identification and removal product for IBM PC and compatible computers which searches for known viruses in the PC's memory, boot sector, and files on fixed or removable disks including 5.25" and 3.5" diskettes. It allows the search of all or selected subdirectories and allows the user to choose how files are backed up before the viruses are removed.

If a virus is detected, VirHUNT can remove the malicious code, overwrite and delete the infected file, or Halt the system to prevent further contamination. The remove option eradicates the virus from the infected file or boot sector. Before using this option, refer to the VirHUNT manual for information on viruses which have removal problems. The wipefile option overwrites the infected file with 0s and afterwards deletes the file. The last option locks up the system instructing the user to power down and reboot from a write protected system disk to search for the infected files.

VirHUNT can also "deactivate" viruses from memory. That is, it will "turn off" memory resident viruses so that re-infection does not occur immediately after removing the virus from an infected file or boot record. Deactivation kills the virus leaving behind the "dead" code in memory.

It has the capability to automatically scan the system every time the system is booted and then returns you to the DOS prompt if no virus are found. If it finds a virus, user intervention is required.

VirHUNT can also store "signatures" of the boot record and files on the system, which allows for previously unknown viruses to be identified and removed.

ASSESSMENT SUMMARY:

VirHUNT was evaluated using a testbed o f approximately 32 viruses which includes the 10 most prevalent viruses affecting Air Force systems. These 10 viruses account for about 90% of the virus incidents reported to AFCSC/SR.

VirHUNT was able to detect 30 out of 32 (94%) viruses, "deactivate" 20 out of 20 (100%) viruses and remove 30 out of 32 (94%) viruses. VirHUNT was not able to detect files infected with our copy of the "Aids" and "Sunday" viruses, although it did detect the Sunday virus when it was active in memory.

USER GUIDANCE:

Always place VirHUNT on a write protected floppy prior to using it to ensure it does not become infected. If using VirHUNT for the first time or for scanning diskettes, use the scan Memory/Boot/Files, all files, and subdirectories options.

If VirHUNT finds a parasitic or a memory resident virus, it may be able to remove the virus from your system. The removal of some viruses is very risky because some viruses overwrite part of the file. Other viruses are impossible to remove from memory once they are active. Refer to the VirHUNT manual for more information on viruses which have removal problems.

VirHUNT uses two different methods for virus removal: wiping (overwriting-deleting) the infected file, and altering (removal of virus) the infected file. If you wish to remove a virus using the first method, select the "Wipe infected files (over-write file, then delete)" option under the virus action screen. This option will overwrite the infected file with 0's and afterward delete the file from your disk. If you wish to use the second method, under the virus action screen, select the "Remove virus from infected file" option. This option attempts to eradicate the virus by removing the virus code from the file. Remember, removing viruses from an infected file does not always work. Also, both of these methods attempt to deactivate memory resident viruses if these are encountered.

If a boot sector virus is detected, there is a good possibility your files have not been damaged, only the boot sector of the disk is infected. Both of the methods mentioned above will remove the virus from the boot sector.

ASSESSED PRODUCT: VIRUSCAN

VENDOR: McAfee & Associates

VERSION: 6.3V72

FINAL USAF-PERC ASSESSMENT REPORT: 90-710 11 February 1991

PRODUCT DESCRIPTION:

VIRUSCAN is a virus detection and identification product for IBM PC and compatible computers which searches for known viruses in the PC's memory, boot sector, partition table, and the files on fixed or removable disks including 5.25" and 3.5" diskettes. After it has identified the virus(es), it has the capability to remove the parasitic virus(es) (viruses that attach themselves to executable files) by first overwriting and then deleting the infected file(s). VIRUSCAN also provides a method of identifying possible infections by unknown (new) viruses. This is done by taking a "picture" of the executable files and critical areas of the disk. Afterward, when a validation check is executed, VIRUSCAN notifies the user if any changes have occurred in the critical areas or in the executable files.

With the /D option, VIRUSCAN removes parasitic viruses by overwriting and then deleting the infected files(s). In addition, VIRUSCAN provides several other options which are:

/A - Scan all files
/D - Overwrite and Delete infected files
/E.xxx - Scan listed overlay extensions
/M - Scan memory for all viruses
/MANY - Scan multiple diskettes
/NLZ - Do not scan inside compressed LZEXE files
/NOMEM - Skip memory scan
/AV - Add validatio n code to specified files
/CV - Check validation codes for files
/RV - Remove validation codes from specified files
/Report d:filename - Create report of infected files
/EXT d:filename - Scan using external virus data files

The VIRUSCAN diskette also contains documentation on how to use this product on a separate file called scanv72.doc and also provides the user with update version notes. The documentation states it can identify 162 known virus strains and 251 virus variants. The viruses that VIRUSCAN can detect are located in an accompanying file called VIRLIST.TXT which contains a virus characteristics list that outlines the

critical features of known IBM PC and PC-compatible viruses that can be identified by this product.

ASSESSMENT SUMMARY:

VIRUSCAN was evaluated using a testbed of approximately 35 viruses which includes the 10 most prevalent viruses affecting Air Force systems. These 10 viruses account for about 90% of the virus incidents reported to AFCSC/SR.

The best results were obtaine d when VIRUSCAN was used with the /A option (scan all files). Even though the /A option requires a substantial amount of time (approximately 50% longer) to complete the scan, it was able to detect **ALL** in the 35 virus testbed and the different scenarios used.

VIRUSCAN is not capable of removing viruses from executable files without deleting the entire file. It does not have the capability to remove boot sector viruses (i.e. "Stoned", "Brain") because they do not attach themselves to executable files. Also, the "picture" taking technique will only notify the user of an infection or possible infection when he performs a validation check on the disk.

USER GUIDANCE:

Always place VIRUSCAN on a write-protected floppy prior to using it to ensure it does not become infected. If using VIRUSCAN for the first time or for scanning diskettes for infected files, use the /A option. Use the /A /D option if you want to also delete any identified virus found on the disk.

For scanning use: scan (drive): /A

Example : scan B: /A

For scanning and removing viruses, use: scan (drive): /A /D

Example: scan B: /A /D

ASSESSED PRODUCT: VSHIELD

VENDOR: McAfee Associates

VERSION: 3.4V79

FINAL USAF-PERC ASSESSMENT REPORT: 90-709 1 Oct 1991

PRODUCT DESCRIPTION:

VSHIELD is a memory resident virus protection/detection product for IBM PC's and compatible computers. It searches for known viruses in the PC's memory, boot sector, partition table, system files and itself before installing in memory. Once in memory, VSHIELD scans all programs executed for known computer viruses. If the program contains a virus, VSHIELD prevents the execution of the program. The user is then instructed to power down the computer and re-boot with a write protected system disk. The computer can then be scanned for viruses. VSHIELD can also check for virus infections by examining the validation code added by VIRUSCAN (scanning program by McAfee & Associates) for modifications. If the validation code has changed, it advises the user a possible virus infection has occurred. Another feature of VSHIELD allows the user to specify which files can and cannot be run by the system. This feature limits the possibility of a virus infection. VSHIELD also has several options for the user to invoke when installing the program. VSHIELD provides the following options:

/CERTIFY filename - Enable access control with exception list
/CHKHI - Check High Memory Area on 286/386 PC's
/CONTACT message - display message when virus i s found
/CV - Check validation codes added by VIRUSCAN
/LOCK - Halt and freeze system when a virus is found
/M - Scan memory for all viruse during installation
/NB - Disable boot sector checking
/NOMEM - Skip memory scan
/REMOVE - Uninstall VSHIELD from memory
/SWAP pathname - Install VSHIELD kernel as memory resident
/F pathname - Required parameter for DOS 2.0 or earlier
/Report d:filename - Create report of infected files
/WINDOWS - Enable checking under Windows

By properly modifying the auto exec.bat file, VSHIELD can automatically scan the system and install itself every time the system is booted. It returns the DOS prompt if no viruses are found. If it finds a virus, user intervention is required.

ASSESSMENT SUMMARY:

Once VSHIELD was installed in memory, it was able to prevent all 64 viruses tested from infecting our systems. The testbed includes the 10 most prevalent viruses affecting Air Force systems. These 10 viruses account for about 90% of the virus incidents reported to AFCSC/SR.

VSHIELD, installed without the /LOCK option, does not prevent viruses from spreading if during the installation there was a virus resident in memory. Depending on the virus, the programs executed will become infected with the virus before VSHIELD can protect them.

USER GUIDANCE:

Place VSHIELD on a write protected floppy before using it to ensure it does not become infected. Also, when installing VSHIELD, recommend using as a minimum the /LOCK and /M options.

If VSHIELD detects a virus in mem ory during installation, immediately power down the system, and re-boot from a write protected system disk. Scan the system with a virus scanning product to detect infected files. Delete the infected files or use a virus eradication program to clean the system from viruses.

3.5 UNIX SECURITY PRODUCTS

ASSESSED PRODUCT: Scrub Pro (part of Unishred Pro)

VERSION: 2.2.4a for Sun Microsystems SPARC systems

VENDOR: Los Altos Technologies, Incorporated

FINAL ASSESSMENT REPORT: 93-502 6 December 1994

PRODUCT DESCRIPTION:

Scrub Pro, part of the Unishred Pro disk declassification software product, is a software program designed to clear or purge and entire Small Computer Systems Interface (SCSI) disks connected to UNIX systems. Scrub Pro allows the user to specify the overwrite pattern and the number of passes to be executed for the clearing and purging functions. It uses low-level SCSI commands to overwrite boot files, super blocks, swap space, alternate cylinders, disk labels, operating system bad blocks, and the partition space allocated to the UNIX file system. Scrub Pro automatically verifies the overwriting process by using write-read-verify operations to detect memory, data bus, or disk parity errors.

Scrub Pro invokes low-level SCSI commands to retrieve and display the manufacture's original defect list and the grown defect list directly from the disk. The grown defect display shows the extent of defects that have occurred after factory release of the disk. This allows the Designated Approving Authority (DAA) to define the acceptable level of data remanence that might exist in grown defect sectors.

Scrub Pro prepares a classification audit report that gives the following information: date, machine name, disk logical name, overwrite pattern used for each pass, program version number, and the program start and completion times. If an error prevents successful operation using the selected clearing or purging procedure, the Scrub Pro program gives an error notification message to warn personnel against improper release of the disk, and ScrubPro suppresses creation of the audit report.

ASSESSMENT SUMMARY:

The Scrub Pro (version 2.2.4a) Object Reuse function was assessed by MITRE and the Product Assessment and Certification Center (PACC) against the overwrite procedures outlined in the Air Force Systems Security Instruction Remanence Security (AFSSI 5020), 15 April 1991. Scrub Pro on a Sun Microsystems SPARC2 running SUN OS 4.1.3 (Solaris 1.1) with an external Hewlett-Packard 1.2 Gigabyte SCSI hard disk,

does not fully implement the AFSSI requirement to overwrite all addressable locations - particularly the bad sectors and the maintenance area. Nevertheless, a DAA may be willing to accept the risk and allow the use of Scrub Pro to clear or purge a SCSI disk as long as: the disk has not developed bad sectors over its lifetime since the last successful overwrite, or, if bad sectors did develop, no classified information was written to them.

RECOMMENDATIONS:

As new SCSI disks are acquired, recommend using Scrub Pro to write to all the data locations with a character such as hex "E5". This way, if a sector becomes unusable during the lifetime of the disk, it is easy to determine if the sector was ever used.

Recommend making a copy of the disk's bad sector growth list (G-LIST) before using the drive for classified processing.

Overwriting steps:

1. Whenever the drive needs to be cleared or purged, obtain a current copy of the G-LIST and compare it to the original one. If the lists are the same, continue with step two. If they are not the came, continue with step three.

2. Use Scrub Pro for clearing or purging the SCSI disk. Select a different character than the initial overwrite character. Verify that the disk did not develop any new bad sectors. If no bad sectors have developed, randomly examine sectors for the overwrite character. If all you see is the overwrite character,the clearing or purging was successful.

3. If the lists are not the same, then there is a possibility of not being able to overwrite classified information. Use Scrub Pro for clearing or purging the SCSI disk.

4. Examine the sectors found in the current G-LIST that were not on the original G-LIST for classified information.

5. If the bad sectors do not contain classified information, examine usable sectors at random for the overwrite character. If all you see is the overwrite character, the clearing or purging was successful.

6. If the bad sectors do not contain classified information, the drive retains the highest classification of the data on the bad sectors until it is degaussed or destroyed using an approved method.

Scrub Pro can be run simultaneously to overwrite more than one disk at the same time. When clearing or purging classified information from a UNIX system with more than one disk, consideration should be given to clearing or purging all disks that contain swap files for programs that have processed classified information.

Overwritten disks must be reformatted using the appropriate operating system supplied reformatting program before the disk can be re-used on a UNIX system. Users should record the disk format and partition information before executing Scrub Pro to simplify reformatting if the disk is to be used on the same or similar computer system.

Chapter 4

POINTS OF CONTACT

Assessor Points of Contact		
Assessor	Contact and Address	Phone
* Air Force Product Evaluation and Resource Center (USAF-PERC)	AFCSC/SRVC Brooks AFB, TX	DSN: 240-2171 (512) 536-2171
# Naval Command, Control and Ocean Surveillance Center In Service Engineering NISE EAST	Susan Morrill 4600 Marriot Dr. Code 421 N. Charleston, SC 29406	DSN: 563-2030 EXT 4460 (803) 974-4460

Vendor Points of Contact		
Vendor	Contact and Address	Phone
# A. Padgett Peterson	P.O. Box 1203 Windermere, FL 34786 Internet: padgett%tccslr.dnet@mmc.com	(407) 352-6007
* AT&T	Guilford Center P.O. Box 20046 Greensboro, NC 27420	(919) 279-5245
* # Central Point Software	Customer Service 15220 N.W. Greenbrier Pkwy Beaverton, OR 97006	(503) 690-8080
* Digital Dispatch, Inc.	Customer Service 55 Lakeland Shores Minneapolis, MN 55432	1-800-221-8091
* Fischer International Systems Corporation	Debra Peterson 4073 Merchantile Avenue Naples, FL 33942	(813) 643-1500
* Hughes Data Systems, Incorporated	Guy Williams 319 S.W. Washington Suite 310 Portland, OR 97204	(503) 243-1029
* Isolation Systems Limited	T. Patrick Bird 26 Six Point Road Toronto, Ontario, M8Z 2W9, Canada	(416) 231-1248
* McAfee Associates	Customer Service 4423 Cheeney St. Santa Clara, CA 95054	(408) 988-3832
* Media Security, Incorporated	Current Address Unavailable	---
* Micronyx, Incorporated	Larry DuBroc John Watson 1910 N. Central Expressway Suite 400 Richardson, TX 75080	(214) 690-0595
* OITC, Inc.	Customer Service P.O. Box 73 Melbourne Beach, FL 32751	(407) 984-3714
* Pan Am World Services	Robert Schild Eastern Space and Missile Center Patrick AFB, FL 32925	(407) 494-7322
* Pyramid Development Corp.	Customer Service 20 Hurlbut Street West Hartford, CT 06110	(203) 953-9832
* Symantec Corp. (formerly Peter Norton	Mary Chacon 10201 Torrie Avenue	1-800-441-7234,

	Symantec Corp. (formerly Peter Norton Computing, Inc.)		
*	Systematic Computer Services	Lloyd A. Greene 3206 Harvard Blvd. Dayton, OH 45406-4126	(513) 275-2937

U.S. Navy (NISE EAST) Assessed Produc ts
* U.S. Air Force (USAF-PERC) Assessed Products

Note: DON procurement officials seeking information about purchasing products can contact vendors directly. All other contact with vendor officials should be made through NISE EAST, Code 043 or USAF-PERC.

APPENDIX A
TRUSTED COMPUTING BASE SKETCHES
[Adapted from DoD 5200.28-STD]

A Trusted Computing Base (TCB) is a collection of hardware, software, and procedures that meet a set of evaluation standards. The National Computer Security Center (NCSC) publishes these standards in DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria, known as the "Orange Book." Evaluated systems that meet a "class" standard receive a TCB Class rating; each class has its own rating criteria.

The Classes. A brief description for each class follows. Note the criteria for each class includes and incorporates **ALL** criteria for the preceding class(es). In increasing "trustworthy" order the classes are:

a. **CLASS D, Minimal Protection**. This lowest class includes operating systems for which there are little or no specific security protection features. This class also includes evaluated systems which do not meet higher class criteria.

b. **CLASS C1, Discretionary Security Protection**. C1 is a primitive TCB with scant Discretionary Access Control protection features that separate users from data. Such a system would be expected to operate in an environment where there are cooperating users who process data at the same sensitivity level. It incorporates some rudimentary controls which enforce access limitations on a group of users basis. Its protection safeguards private or project information and prevents users from accidentally reading and destroying each other's data. This class may not be used for DON systems as it fails to meet minimum DoD security policy requirements.

c. **CLASS C2, Controlled Access Protection**. C2 is a basic TCB which provides intermediate-level Discretionary Access Control protection features. These features more clearly distinguish user actions through log-in identification and authentication, auditing security-relevant events, isolating data, and resource protection capabilities. C2 TCBs significantly improve upon the C1 level by ensuring users are individually accountable for their actions and that residual information cannot be accessed. This class is the minimum TCB class authorized for DON multiuser systems.

d. **CLASS B1, Labeled Security Protection**. B1 is an intermediate-level TCB which provides elementary-level Mandatory Access Control protection features, as well as intermediate-level Discretionary Access Control features. Class B1 is the first TCB class which implements Mandatory Access Control upon users and data based on the user's clearance versus the data's sensitivity. Data

must be labeled and all users given explicit permission to access that data. Sensitivity labels make access-control decisions based on an informal security policy model that states the rules for how named subjects (users, programs) may access named objects (files, records).

e. **CLASS B2, Structured Protection**. B2 is an enhanced-level TCB which provides intermediate-level Mandatory Access Control protection features, as well as enhanced Discretionary Access Control features. Its sensitivity labels allow for enforcing access-control decisions based on a formally specified security policy model that documents rules for how each subject (users, programs) may access each object (files, records). The protection features must show carefully separated protection-critical and non-protection-critical elements. Class B2 requires additional internal protection mechanisms that prevent information "leakage" through hidden, or covert, signal channels. Class B2 also provides operational support features, such as System Security Officer (SSO) and System Administrator (SA) functions. Stringent configuration management practices also apply.

f. **CLASS B3, Security Domains**. B3 is an advanced TCB which provides highly effective Discretionary and Mandatory Access Controls. These controls must implement the "reference monitor concept" through correspondence to a formally specified security policy model. Significant security and software engineering during the design, testing, and implementation phases to achieve the required level of confidence, or trust, are also requirements. Operational support features extend auditing capabilities as well as provide System Security Officer (SSO) functions needed for a trusted system recovery.

g. **CLASS A1, Verified Design**. A1 is a highly advanced TCB which provides exceptionally effective Discretionary and Mandatory Access Controls that are identical to those of Class B3 TCB systems. Here, however, formal analyses prove that the design and its implementation are rigorous (in the mathematical sense) using a Formal Top Level Specification as documentation. Extended operational support features provide techniques for trusted system distribution to deployed sites.

The Criteria. DoD 5200.28-STD cites the specific criteria for each TCB Class. The criteria build upon four fundamental security principles, as discussed in the next several paragraphs.

a. **Security Policy**. Security policy statements govern the manner in which sensitive information or classified information must be protected according to U.S. statutes.

(1) Discretionary Access Controls (Class C1 and Above). This is the need-to-know concept. These controls enforce rules for sharing data among users.

(2) Object Reuse (Class C2 and Above). The main memory or mass storage area accessed by a subject must not have any residual data for which the subject does not have access authorization.

(3) Labels (Class B1 and Above). Within a TCB, labels represent the sensitivity or security level. A subject's label represents its clearance level and need-to-know privileges. An information object's label indicates the actual sensitivity of the information, while a storage object's label indicates the sensitivity of the data it currently holds.

(4) Label Integrity (Class B1 and Above). Sensitivity labels must correspond exactly to the sensitivity level of the associated subject or object. Labels must be TCB-protected against tampering or unauthorized alteration.

(5) Exchanging Labeled Information (Class B1 and Higher). Exchanging (e.g., importing or exporting) information between the TCB and a communications channel or device requires the TCB to track which are multilevel and which are single level devices.

n MultiLevel (Class B1 and Above). For multilevel situations, the TCB ensures that an object's sensitivity is within the range permitted by exchanging both the object and its sensitivity label.

n Single-Level Devices (Class B1 and Above). For a single-level, the exchange involves only the object itself, since the sensitivity level is "fixed" and known in advance. The TCB will only allow exchanges at that level to occur.

(6) Labeling Human-Readable Output (Class B1 and Above). Human-readable output must be marked with a plain language version of the object's sensitivity level to alert people who will handle the information about its sensitivity (e.g., English language security classification banner at the top and bottom of each page).

(7) Mandatory Access Controls (Class B1 and Above). These controls enforce rules that govern which subjects (e.g., users, programs) may access (e.g., read, write, change, delete) which specific objects (e.g., data). A subject's clearance level must always be consistent with an object's sensitivity level. Thus, a subject at a specific sensitivity level may read from an area (e.g., main memory) with an equal or lesser sensitivity level, and may write to an area with an equal or greater sensitivity level.

(8) Subject Sensitivity Labels (Class B2 and Above). During an interactive session, the TCB must keep the terminal user informed about changes in the "current working security level." Terminal users may display the complete sensitivity label for processes they are using.

(9) Device Labels (Class B2 and Above). The TCB must track the minimum and maximum security level assignments for all physically attached devices (e.g., terminals, printers). These assignments are often called "classmarks" for the device.

b. **Accountability**. Accountability is the ability to determine who did what, to whom, when, and under what conditions.

(1) Identification and Authentication (Class C1 and Above). Users must identify themselves (e.g., provide user-ids) to the system and the TCB must authenticate their identity (e.g., passwords) prior to granting access to the system.

(2) Audit (Class C2 and Above). The TCB must record all security-relevant events (e.g., changes to device classmarks) in a TCB-protected area called the audit trail.

(3) Trusted Path (Class B2 and Above). The TCB must provide a means to clearly identify itself to the user. This ensures the user's dialogue is with the TCB and not with a masquerading program that may be attempting to "steal" passwords, for example.

c. **Assurance**. Assurance pertains to the steps taken to correctly implement the security policy.

(1) System Architecture (Class C1 and Above). The system architecture must separate TCB processes (e.g., reference monitor) from user processes (e.g., applications programs). The system architecture must also separate each user's data from every other user's data.

(2) System Integrity (Class C1 and Above). Periodic validation checks must ensure the security mechanisms function properly and correctly. These features can either be automated, or manually invoked by the System Operator.

(3) Security Testing (Class C1 and Above). The range and depth for security testing increases for each class. Test results affirm security protection features have been correctly implemented.

(4) Design Specification and Verification (Class B1 and Above). The security policy enforced by the TCB must be informally (i.e., non-mathematically) structured or formally (i.e., mathematically) modeled. At higher TCB classes, the mathematical modeling becomes more rigorous (e.g., from "show" fidelity, to "convincing argument" or demonstration, and onward to "mathematical proof"). The requirement for correspondence between the policy model and the design specifications (e.g., Descriptive Top Level Specification (DTLS), Formal Top Level Specification (FTLS)) also increases.

(5) Covert Channel Analysis Results (Class B2 and Above). Covert channels are unintended signaling paths which can bypass the TCB's access controls. The analysis must identify these channels, show how to minimize their bandwidth, and audit their use.

(6) Trusted Facility Management (Class B2 and Above). TCB features must define and support separate System Operator and System Administrator functions. The System Operator has fewer security-relevant privileges than does the System Administrator. Both are "Trusted Officials", though, and have the skills and opportunity to circumvent the system's security enforcement mechanisms, but their trustworthiness is such that they are unlikely to do so.

(7) Configuration Management (Class B2 and Above). These are the procedures used to establish a baseline and control changes throughout the system's life-cycle. Configuration management becomes more comprehensive as the TCB class increases.

(8) Trusted Recovery (Class B3 and Above). There must be procedures available which preserve security protection integrity and return the system to a secure processing environment after a failure.

(9) Trusted Distribution (Class A1). There must be a "high confidence" system for distributing each TCB version which ensures its integrity upon receipt at each site.

d. **Documentation**. Documents that describe the TCB's objectives (security policy), design, performance, and operation must be prepared, approved, and published.

(1) Security Features User's Guide (Class C1 and Above). This Guide is for system users. It describes the security protection features provided by the TCB, gives guidelines on their use, and explains how they interact with each other. The Guide also describes expected system reaction to security-relevant events (e.g., access violations, incorrect password).

(2) Trusted Facility Manual (Class C1 and Above). This Manual is for the System Administrator, Security Officer, and System Operators. It gives detailed information about the security protection features provided by the TCB and describes how to use them. It also describes their limitations, or restrictions, and gives authoritative information about how to establish and maintain a secure operational environment.

(3) Test Documentation (Class C1 and Above). Provides the plans and documents results for testing the TCB's security protection features. The range and depth increase as the TCB class increases.

(4) Design Documentation (Class C1 and Above). Depending on the TCB class, design documentation requirements vary considerably. It ranges from a simple statement, to a mathematically based description, to detailed proofs and correspondence, up to a Security Policy Model and its proof.

APPENDIX B
NCSC EVALUATED PRODUCTS

Serial No. CSC-EPL-84/002

EVALUATED PRODUCT: Access Control Facility 2 (ACF2)

VENDOR: SKK, Inc.

VERSIONS: ACF2 Release 3.1.3

DATE: 3 August 1984

OVERALL EVALUATION CLASS: C2

PRODUCT DESCRIPTION:

The ACF2 security subsystem is designed to provide security for data stored on computer systems using the IBM MVS or VSI operating systems. ACF2 provides protection by default for data sets resident on Direct Access Storage Devices (DASDs), IBM 3850 Mass Storage System (MSS) and tape volumes. Protection levels of READ, WRITE, ALLOCATE (allocation, rename, scratch and catalog functions) and EXECUTE-only are supported. Interfaces between ACF2 and many popular commercial software products are provided by SKK. These software products include Information Management System (IMS) and Customer Information Control System (CICS) by IBM.

EVALUATION SUMMARY:

The security protection provided by SKK's Access Control Facility 2 (ACF2) Release 3.1.3 running with Multiple Virtual Storage/System Product (MVS/SP) 1.3.3 operating system has been evaluated by the Department of Defense Computer Security Center (DoDCSC). The security features of the ACF2/MVS were tested against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria (the Criteria), dated 15 August 1983.

The DoDCSC evaluation team has determined that the highest class at which ACF2/MVS satisfies all the specified requirements of the Criteria is class C2.

The overall system integrity level of the ACF2/MVS is C2. ACF2/MVS can not meet higher levels of the Criteria without significant modification or reimplementation of a major fraction of MVS and its supporting subsystems.

The evaluation of ACF2 was conducted on the MVS operating system only. The integrity of ACF2 is dependent upon the integrity of the MVS system itself.

The rating given to the evaluated system (viz., C2) is the highest level of the Criteria at which the system satisfies all the specified requirements. The "range of feasible

use" is intended to convey the overall system integrity level of the system as it is delivered by the vendor and indicates that this system could be used in an environment requiring an evaluation class within this range so long as the missing features are not essential to the operational capability.

For a complete description of how ACF2/MVS satisfies each requirement of the Criteria, see Final Evaluation Report, SKK Access Control Facility 2 (ACF2), Release 3.1.3 (Report No. CSC-EPL-84/002).

Serial No. CSC-EPL-94/001

EVALUATED PRODUCT: Amdahl UTS/MLS

VENDOR: Amdahl Corporation

VERSION EVALUATED: UTS/MLS Release 2.1.5+

EVALUATION DATE: 7 January 1994

OVERALL EVALUATION CLASS: B1 (TCSEC)

PRODUCT DESCRIPTION:

Amdahl Corporation's UTS/MLS 2.1.5+ is a multi-level secure version of Amdahl UTS* 2.1.5+, a UNIX** System V compatible product. UTS/MLS is a multi-user, multi-tasking operating system that can support up to 65,000 users. UTS/MLS maintains System V application compatibility and the vendor claims it is compatible with the System V Interface Definition (SVID).UTS/MLS has been evaluated on the Amdahl 5990 and 5995 mainframes, which provide the System 370/XA architecture.

In addition to using the traditional protection mechanism of the UNIX operating system to provide discretionary access control, UTS/MLS also provides mandatory access controls to restrict the flow of information based on the sensitivity of the information and the clearances of the users attempting to access the information. The mandatory security policy is consistent with the Bell-La Padula model and conforms with DoD policy. UTS/MLS provides a flexible labeling scheme that supports up to 255 hierarchical classification levels and 1024 nonhierarchical categories. Discretionary controls are applied to files, directories, named pipes, device special files, symbolic links, shared memory, message queues, and semaphore sets. Mandatory controls are applied to the same set of objects, as well as to processes, line printer queue entries, at (1S) queue entries, and mail messages. UTS/MLS does exempt objects from protection; for details, see the Final Evaluation Report.

The administrator has the capability to restrict users and login ports to selectable classification ranges. A multi-level mail capability allows users to communicate with each other at classifications defined by the administrator. UTS/MLS enforces a security policy that prevents both the unauthorized declassification of information and unauthorized modification of trusted code. The mandatory access controls are implemented by extending the meaning of the traditional UNIX group fields. Other commands have been added to allow users to create UNIX groups on the system. Users can change levels without having to logout. The discretionary policy uses the traditional UNIX Owner/Group/Other permission bit mechanism.

A random password generator implements the algorithms recommended in the DoD Password Management Guideline, CSC-STD-002-85. Audit trail records are generated for security-relevant events and can be analyzed by an administrator using an audit trail formatter. A trusted path is provided at login time to ensure that users are communicating with the TCB. A secure interprocess communication mechanism allows

trusted server processes to reliably obtain identification and clearance information of client processes that submit messages to the server.

EVALUATION SUMMARY:

The security protection provided by Amdahl Corporation's UTS/MLS 2.1.5+, configured according to the most secure manner described in the Trusted Facility Manual, has been evaluated by the National Security Agency (NSA) against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) [DOD 5200.28-STD] dated December 1985.

The NSA evaluation team has determined that the highest class at which UTS/MLS satisfies all specified requirements of the TCSEC is class B1. A system that is rated as being a B1 class system provides a Trusted Computing Base (TCB) that preserves the integrity of sensitivity labels, and uses them to enforce a set of mandatory access control rules. B1 systems also provide discretionary access controls, identification and authentication, object cleansing between reuse, and auditing facilities. Assurance is provided primarily through architectural analysis and testing.

UTS/MLS also provides some features and assurances beyond those required for a class B1 system; specifically, it has been found to satisfy B2 Subject Sensitivity Labels, B2 Device Labels, and B2 Trusted Path requirements. This product is also participating in the NSA Rating Maintenance Program (RAMP). For a complete description of how UTS/MLS satisfies each requirement of the TCSEC, see Final Evaluation Report, Amdahl Corporation UTS/MLS 2.1.5+.

* UTS is a trademark of Amdahl Corporation.
** UNIX is a trademark of Unix System Laboratories, Inc.

Serial No. CSC-EPL-94/005

EVALUATED PRODUCT: AOS/VS II

VENDOR: Data General Corporation

VERSION: Release 3.01

DATE: 1 June 1994

OVERALL EVALUATION CLASS: C2

PRODUCT DESCRIPTION:

The AOS/VS II system is the newest development in the operating system software for Data General's ECLIPSE MV/Family computers. AOS/VS II is a general-purpose timesharing system for use in a wide range of applications. The evaluated hardware ranges from the MV / 1000DC, a small desktop machine,to the MV / 6000HA, a large (6-CPU) multiprocessor. AOS/VS II provides virtual memory, a hierarchical file system, and a ring-based protection structure for the operating system and for trusted applications. The evaluated AOS/VS II product does not include networking and distributed processing capabilities.

AOS/VS II provides discretionary access controls between users and objects through the use of ACLs. An ACL contains a list f user names and group names along with the access rights to the object. Any combination of user names, group names, and access rights (including null access) may be specified in an ACL. A user group is a set of users, associated by group name. Groups offer a simple way to handle access control for projects, since users can gain access to files by group name, as well as by user name. The main benefit of groups is that their use can eliminate the maintenance of long and intricate ACLs.

AOS/VS II will not perform any action on behalf of a user until the user has logged on. In order to log on, the user must provide a unique user name as identification and must provide the correct password associated with the user name for authentication. Passwords are 6 to 15 characters in length and are composed of any printable character. The system administrator may specify a different number of logon tries allowed from 1 to 10, and may also disable the local console line after a given number of logon tries (five logon tries is the default). The last interactive logon time is displayed on screen with each new logon session.

Information about users, such as privileges and passwords, are stored in user profiles. All user profiles have null access control lists, which means that only

processes which have the Super user privilege set on can read or change the user profiles. User passwords can be encrypted before they are stored.

AOS/VS II ensures that storage objects do not contain residual data upon reallocation and that access rights to the storage objects have been removed. Storage objects include: filesystem caches, memory pages, shared pages, filesystem objects, and disk devices.

AOS/VS II provides the ability to keep a log of security-relevant system events in audit files. To become an authorized administrator for auditing, a user must have either the System Manager privilege turned on or have physical access to the system console. An administrator can access a software switch that provides two extra security features: the audit files can only be written to by the kernel; and logging can only be stopped by a system power down.

EVALUATION SUMMARY:

The security protection provided by AOS/VS II, configured according to the most secure manner described in the Trusted Facility Manual, has been evaluated by the National Security Agency (NSA) against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) [DoD 5200.28-STD] dated December 1985.

The evaluation team has determined that the highest class at which AOS/VS II satisfies all specified requirements of the TCSEC is class C2. A system that is rated as being a C2 class system provides a Trusted Computing Base (TCB) that implements user identification and authentication to control general system access, discretionary access control to protect objects and allow owners to distribute access to those objects as appropriate, and auditing to enforce general user accountability.

In addition to the AOS/VS II Version 3.01 features that meet the C2 TCSEC requirements, two functional aspects of higher level requirements are met: B3 discretionary access control (DAC), and B1 system architecture.

This product is also participating in the NSA Rating Maintenance Program (RAMP). For a complete description of how AOS/VS II satisfies each requirement of the TCSEC, see Final Evaluation Report, Data General Corporation AOS/VS II (CSC-EPL-94/005).

Serial No. CSC-EPL-92/005

EVALUATED PRODUCT: Boot Protection Subsystem

VENDOR: Krypton Corp.

VERSION: Boot Protection Subsystem version 1.91

EVALUATION DATE: 10 April 1992

OVERALL EVALUATION CLASS: I&A / D1

PRODUCT DESCRIPTION:

The Boot Protection Subsystem is designed to provide password protection for microcomputer resources. The hardware base of Boot Protection Subsystem consists of an EPSOM card that is inserted in an IBM-PC, IBM-XT, IBM-AT, or other compatible computer. The software portion of the product is installed by running the installation utility provided with the system.

The Boot Protection Subsystem requires that a user provide a six-character id and a password before the machine will enter its boot cycle. It keeps track of the number of times a given password has been used, and will lock the user out if it exceeds a pre-set threshold. In addition, once logon is complete, a warning banner will give notice of any unsuccessful logon attempts or approaching password expiration.

EVALUATION SUMMARY:

The Trusted Product and Network Security Evaluations Division of the National Security Agency (NSA) has evaluated the security protection provided by the Boot Protection Subsystem. The security features for Identification and Authentication were evaluated against the requirements specified by the Computer Security Subsystem Interpretation (CSSI) of the DoD Trusted Computer System Evaluation Criteria (TCSEC).

An I&A subsystem requires users to identify themselves to it before any other actions may be performed. A subsystem rated as an I&A/D1 system must provide a unique identifier and authenticator for each user or group of users, and use those items to control access to system objects. The Boot Protection Subsystem requires each user to submit the correct group name and password. If it is not correctly supplied, the system will not enter its boot cycle, thus blocking all access to system resources. An I&A subsystem must also protect authentication data so that it cannot be accessed by any unauthorized user. The Boot Protection Subsystem sufficiently protects the authentication data. The final evaluation rating is therefore D1.

For a complete description of how the Boot Protection Subsystem system satisfies each requirement of the CSSI, see the "Final Evaluation Report, Krypton Boot Protection Subsystem" (Report No.CSC-EPL-92/005).

Subject: EPL Evaluated CMWs Serial No. CSC-EPL-91/002

EVALUATED PRODUCT: Compartmented Mode Workstation Plus (CMW+) Version 1.0

VENDOR: SecureWare, Inc.

EVALUATION DATE: 30 January 1991

EVALUATION CLASS: B1

PRODUCT DESCRIPTION:

SecureWare's Compartmented Mode Workstation Plus (CMW+) Version 1.0 is a multilevel secure version of Apple Computer's A/UX (1) Release 1.1 for the Macintosh IIx and Macintosh IIcx (2) workstations. It incorporates trusted versions of the X Window System Version 11, Release 3 (11R3) and the OSF/Motif Window Manager 1.0. CMW+ is a general-purpose, multi-tasking operating system with a windowing environment. It adds the security and functional enhancements required by the Trusted Computer System Evaluation Criteria (TCSEC) to A/UX, the X Window System (3) and the OSF/Motif (4) Window Manager.

CMW+ is designed to provide security for environments requiring trusted desktop data processing. In addition to providing the traditional user specified access controls (i.e., discretionary access controls) through protection bits, CMW+ provides access control lists, which provide a more flexible user specified access mechanism, and mandatory access control, to control the distribution of information protected by the system to only those users who have been authorized for the information. The mandatory security policy is consistent with the Bell-La Padula model and conforms with Department of Defense policy. In addition, CMW+ provides an information labeling policy on the information contained in objects. A virtually unlimited number of classifications and compartments are supported.

CMW+ provides user identification and authentication through user names and passwords, and individual accountability through its auditing mechanisms. The authentication features of CMW+ comply with the guidelines recommended in the DoD Password Management Guideline, CSC-STD-002-85. The auditing mechanism is controlled from a Motif-based interface and supports pre and post-selection by user, group, event and sensitivity level range. A trusted X server and trusted Motif window manager provide a trusted path mechanism for login and for performing security-relevant functions. The security policies have been implemented using X protocol extensions in a binary backwards-compatible manner.

The system supports three separate privileged user roles as defined in the CMWREQs for maintaining the system: System Administrator, Information System Security Officer (ISSO) and Operator. Motif-based programs are provided for the System Administrator and ISSO to enable them to easily administer the audit subsystem, user accounts and the device subsystem. CMW+ supplies a privilege mechanism and a number of discrete privileges that may be used to implement the principle of least privilege. CMW+ also supports configurable command authorizations on a per user basis to limit access to various commands. CMW+ is delivered with a number of programs which may be used to reduce the likelihood of data compromise in the event of a system failure.

CMW+ can transfer data, including all security attribute information, to and from other SecureWare based systems via removable media. SecureWare has designed CMW+ to be compatible with many other systems that are available in the marketplace.

EVALUATION SUMMARY:

The security protection provided by the SecureWare Compartmented Mode Workstation Plus (CMW+) operating system running on the Apple Macintosh IIx or IIcx workstations, configured as described in the CMW+ Trusted Facility Manual, has been evaluated against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria [DOD 5200.28-STD], dated December 1985.

The evaluation team has determined that the highest class at which SecureWare CMW+ satisfies all the specified requirements of the Criteria is class B1. In addition, SecureWare CMW+ satisfies the functionality of the B2 requirement for Configuration Management, the B3 requirements for DAC, Trusted Path, Trusted Facility Management, Trusted Recovery, and the A1 requirement for Trusted Distribution.

In conjunction with the TCSEC evaluation, CMW+ was also evaluated against the Compartmented Mode Workstation requirements of the Security Requirements for System High and Compartmented Mode Workstations. See the entry in the TCB Extensions List for more information.

For a complete description of how SecureWare CMW+ satisfies each requirement of the TCSEC, see Final Evaluation Report, Secure Ware Inc., CMW+ (Report CSC-EPL-91/002). In addition, the report should also be consulted for the complete lists of evaluated hardware and software components.

1 UX is a trademark of Apple Computers Inc.

2 Apple and Mcintosh are registered trademarks of Apple Computers, Inc.

3 The X Window System is a trademark of Massachusetts Institute of Technology

4 OSF/MOTIF and MOTIF are trademarks of Open Software Foundations, Inc.

Serial No. CSC-EPL-91/004

EVALUATED PRODUCT: COMPSEC-II

VENDOR: American Computer Security Industries, Inc.

VERSION: COMPSEC-II USA American Version, release B3.1

EVALUATION DATE: 10 June 1991

OVERALL EVALUATION CLASS: I&A / D
AUD / D
DAC / D
OR / D

PRODUCT DESCRIPTION:

COMPSEC-II is a combined hardware and software based product for use in microcomputers. The hardware base of COMPSEC-II consists of a hardware card that is inserted in an IBM-PC,IBM-XT, IBM-AT, 386-based machine, or a 100% compatible computer running DOS versions 2.0 through 3.3. The software portion of the product is installed by running the installation utility provided with the system.

COMPSEC-II provides System Operator utilities to customize the system including initializing users and setting passwords, setting user access to the hardware resources (hard disk,external disk drive), setting user access to files and directories, configuring the audit utility, and activating object reuse. Use of the System Operator utilities requires an additional identification and authentication step.

EVALUATION SUMMARY:

The Trusted Product and Network Security Evaluations Division of the National Security Agency (NSA) has evaluated the security protection provided by COMPSEC-II. The security features for Identification and Authentication, Audit, Discretionary Access Control, and Object Reuse were evaluated against the requirements specified by the Computer Security Subsystem Interpretation (CSSI) of the DoD Trusted Computer System Evaluation Criteria (TCSEC).

An I&A subsystem requires users to identify themselves to it before they do anything on the system. A subsystem rated as an I&A/D2 system must provide a unique identifier and authenticator for each user and use those items to control access to system objects. Additionally, the subsystem must

provide for audit logging of security relevant I&A events and protect the authentication data so that it cannot be accessed by any unauthorized user.

COMPSEC-II requires individual users to identify themselves and authenticate their identity before they are allowed access to the system. COMPSEC-II audits the occurrence of all security relevant I&A events. However, COMPSEC-II fails to sufficiently protect the authentication data from unauthorized access.

An audit subsystem must be capable of recording all security relevant actions that occur on the system. The record of these events must be protected from modification or unauthorized access or destruction. COMPSEC-II fails to audit the security relevant actions taken by the system administrator during the configuration and update of the System Operator utilities mentioned above in the Product Description. Additionally, COMPSEC-II fails to sufficiently protect the audit log data from unauthorized access.

A DAC/D2 subsystem uses the identification of subjects and objects to determine whether users are authorized for each access attempt. The DAC subsystem must provide the capability for users to specify how other users or groups may access the objects they control. Audit data must be generated that records access mediation events. Propagation of access rights must be limited to authorized users. The DAC mechanism must deny access to an object when no explicit action has been taken to allow access.

If COMPSEC-II is configured for Master Exclusion Access Control as described in the vendor's operations manual, then COMPSEC-II satisfies the functional requirements for DAC at the D2 level.

An OR/D2 subsystem requires that all authorizations to the information contained within a storage object shall be revoked prior to assignment or allocation to a subject. COMPSEC-II overwrites file system objects upon deallocation and clears memory objects at the end of a user's session. COMPSEC-II satisfies the functional requirements for OR at the D2 level.

In addition to meeting the functional requirements, subsystems must also meet the assurance and documentation requirements of the CSSI. COMPSEC-II failed to satisfy the assurance and documentation requirements and therefore receives a composite rating of D for each of the four features that were evaluated.

For a complete description of how the COMPSEC-II system satisfies each requirement of the CSSI, see the "Final Evaluation Report, American Computer Security Industries, Inc., COMPSEC-II" (Report No. CSC-EPL-91/004).

Serial No. CSC-EPL-92/004

EVALUATED PRODUCT: ConvexOS/Secure

VENDOR: CONVEX Computer Corporation

VERSION EVALUATED: V10.0

EVALUATION DATE: 29 May 1992

OVERALL EVALUATION CLASS: C2

PRODUCT DESCRIPTION:

ConvexOS/Secure is a secure version of ConvexOS, which is an enhanced implementation of 4.2 BSD and 4.3 BSD UNIX. ConvexOS/Secure is designed to comply with more stringent requirements for data and system security than that provided by standard UNIX services. This trusted version of ConvexOS is available for all CONVEX C2 series and C3 series supercomputer systems. ConvexOS/Secure preserves the symmetric multiprocessing, automatic vectorizing and parallelizing capabilities of the CONVEX system.

ConvexOS/Secure is designed to provide security for environments requiring trusted, high-performance computing services. In addition to providing the traditional UNIX user-specified access controls (i.e., discretionary access controls) through protection bits, ConvexOS/Secure provides access control lists, which provide a more flexible user specified access control mechanism. Access controllists allow users to grant or deny access to the granularity of an individual user.

ConvexOS/Secure provides user identification and authentication through a valid login user name and password. The identity of the user is preserved by use of an immutable login user identifier associated with the user account and all processes that the user creates. The password database has been restructured to prevent unauthorized users from accessing the encrypted password information. The authentication features of ConvexOS/Secure comply with many of the guidelines recommended in the DoD Password Management Guideline, CSC-STD-002-85.

Individual accountability is provided through the auditing mechanism. System audit trail records are maintained that record the user's identity, date, time, terminal identification and type of activity. Unsuccessful login attempts, file accesses and resource denials are included in the audit trail. The auditing mechanism supports pre- and post-selection by user, group, type of event, start/end time and filename.

ConvexOS/Secure supplies a privilege mechanism and a number of discrete privileges to control access to and creation of setup programs and access to the auditing subsystem. Authorizations can be granted on a per user basis to either allow or grant access to various administrative commands.

ConvexOS/Secure controls object reuse by clearing all newly allocated storage or preventing reading of a storage object before it is written. ConvexOS/Secure supports a

boot time tunable parameter to overwrite file contents on disk with a specified pattern at the time a file is deleted.

ConvexOS/Secure employs a hardware-enforced, five ring segmentation of virtual memory. User code and data reside in the upper ring, with the operating system code and data buffers residing in the lower four rings. Virtual memory hardware ensures process isolation by assigning each process its own address space. One process cannot access another address space except through a standard shared memory mechanism.

EVALUATION SUMMARY:

The security protection provided by ConvexOS/Secure has been evaluated by the National Security Agency (NSA). The security features of Convex OS/Secure were tested against the requirements specified by the``Department of Defense Trusted Computer System Evaluation Criteria" dated December 1985. The NSA evaluation team has determined that the highest class at which ConvexOS/Secure satisfied the requirements set forth in the TCSEC was C2.

For a complete description of how ConvexOS/Secure satisfies each requirement of the Criteria, see Final Evaluation Report, CONVEX Computer Corporation, ConvexOS/Secure (Report No. CSC-EPL-92/004).

Serial No. CSC-EPL-93-006

EVALUATED PRODUCT: CX/SX

VENDOR: Harris Computer Systems Division

VERSION EVALUATED: Release 6.1.1

EVALUATION DATE: 15 September 1993

OVERALL EVALUATION CLASS: B1

PRODUCT DESCRIPTION:

CX/SX Version 6.1.1 is an extension of Harris' UNIX* based CX/UX operating system that runs on the Series 4000 Night Hawk product line. The Night Hawk 4000 series is a multiprocessor system based on the Motorola 88100 reduced instruction set computer processor. Models in the series allow from one to eight processors. A dual bus architecture is used to interface with memory, controllers and peripherals to ensure high system throughput. CX/SX is a multi-threaded, fully-preemptive operating system that takes advantage of the Night Hawk's processor configuration for high performance, secure computing applications.CX/SX was created by incorporating AT&T's System V/MLS features into CX/UX in addition to security functionality developed by Harris.

CX/SX is designed to be software compatible with CX/UX while adding additional security features. CX/SX provides the traditional UNIX user-specified access controls of protection bits for discretionary access control. Commands have also been added to allow users to dynamically create discretionary groups on the system. Mandatory access controls are provided to limit the distribution of information only to authorized users. CX/SX provides a flexible labeling scheme with capability for 255 hierarchical levels and 1024 non-hierarchical categories. The CX/SX mandatory access control policy is consistent with the Bell-LaPadula security policy model. The CX/SX security policy also prevents the unauthorized declassification of user information and unauthorized modification of trusted code.CX/SX provides for user identification and authentication through user identifiers and passwords. The passwords are created by a random password generator. Audit trails of security relevant activities are generated to allow the system administrator to determine individual accountability for actions taken on the system. CX/SX allows secure object reuse by clearing resources on allocation or deallocation, as appropriate for the object and security policy.

CX/SX provides additional security features not required of B1 level systems. Login sessions may be restricted to selected classification ranges as specified by the system administrator. Device label ranges are supported allowing specific devices to be constrained to store/receive restricted classifications of data. The system provides subject sensitivity labels and users can determine their security level any time during an interactive session. The CX/SX assurance system provides a mechanism for validating the integrity of the trusted computing base (TCB) and restoring a previously saved TCB.

CX/SX is being maintained under configuration management in accordance with the NCSC Ratings Maintenance Program and it is anticipated that CX/SX will continue to be maintained in accordance with this program.

EVALUATION SUMMARY:

The security protection provided by CX/SX, when configured in a secure manner as described in the Trusted Facility Manual, has been evaluated by the National Security Agency (NSA) against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria [DOD 5200.28-STD] dated December 1985.

The NSA evaluation team has determined that the highest class at which CX/SX satisfies all the specified requirements of the Criteria is class B1. For a complete description of how CX/SX satisfies each requirement of the Criteria, see Final Evaluation Report, Harris Computer Systems CX/SX Version 6.1.1 and LAN/SX Version 6.1.1 (Report CSC-EPL-93/006,007). In addition, the report should also be consulted for the complete lists of evaluated hardware and software components.

* UNIX is a registered trademark of UNIX System Laboratories Incorporated.

Serial No. CSC-EPL-93/007

EVALUATED PRODUCT: CX/SX with LAN/SX

VENDOR: Harris Computer Systems Division

VERSION EVALUATED: Release 6.1.1

EVALUATION DATE: 15 September 1993

OVERALL EVALUATION CLASS: B1 MDIA Network Component

PRODUCT DESCRIPTION:

CX/SX Version 6.1.1 is an extension of Harris' UNIX* based CX/UX operating system that runs on the Series 4000 Night Hawk product line. The NightHawk 4000 series is a multiprocessor system based on the Motorola 88100 reduced instruction set computer processor. CX/SX is a multi-threaded, fully-preemptive operating system that takes advantage of the NightHawks processor configuration for high-performance, secure computing environments. CX/SX was created by incorporating AT&T's System V/MLS features into CX/UX in addition to security functionality developed by Harris. CX/SX provides mandatory access controls, discretionary access controls, identification and authentication of users, auditing of security relevant events, and object reuse.

The LAN/SX Version 6.1.1 network subsystem provides a general purpose frame work for secure network services. LAN/SX can be run over either Harris Ethernet frame-level software or the Verdix Security Local Area Network. LAN/SX adds security features to the Harris Ethernet TCP/IP software. LAN/SX provides an interface to network services, a protocol layer used for communication, and device drivers for control of network devices.

LAN/SX provides mandatory access controls to limit user and host access to network interfaces. The mandatory access control policy is a lattice-based security policy. LAN/SX supports both single-level and multi-level connections on a standard Ethernet interface. Multi-level connections occur via Internet Protocol (IP) security options. Single-level connections occur using the standard IP protocol without security options. The IP security options supported are Commercial Internet Protocol Security Option (providing 255 classification levels and 512 categories) and the Internet Protocol Security Option/Basic Security Option (providing four classification levels). LAN/SX also supports a host-to-host discretionary access control policy allowing a network administrator to control which hosts may be accessed through the network interfaces.

Users accessing the CX/SX system through LAN/SX must use a trusted network application and must pass identification and authentication checks before accessing any resources on the system. LAN/SX produces audit records of security relevant events related to the use of the network subsystem and passes the records onto the CX/SX auditing subsystem for an integrated system audit trail.

CX/SX with LAN/SX is designed to be one partition in a total network system trusted computing base (NTCB). The NTCB partition contains the CX/SX operating

system, a Night Hawk 4000 series machine, and LAN/SX. Ftp, telnet, and rlogin are provided as trusted network applications.

CX/SX is being maintained under configuration management in accordance with the NCSC Ratings Maintenance Program and it is anticipated that CX/SX will continue to be maintained in accordance with this program.

EVALUATION SUMMARY:

The security protection provided by CX/SX with LAN/SX, when configured in a secure manner as described in the Trusted Facility Manual, has been evaluated by the National Security Agency (NSA) against the requirements specified by the Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria (TNI), 31 July 1987, NCSC-TG-005,
Version 1.

The NSA evaluation team has determined that the highest class at which CX/SX with LAN/SX satisfies all the specified requirements of the Criteria is class B1. For a complete description of how CX/SX with LAN/SX satisfies each requirement of the Criteria, see Final Evaluation Report, Harris Computer Systems CX/SX Version 6.1.1 and LAN/SX Version 6.1.1 (Report CSC-EPL-93/006,007). In addition, the report should also be consulted for the complete lists of evaluated hardware and software components.

*: UNIX is a registered trademark of UNIX System Laboratories Incorporated.

Serial No. CSC-EPL-94/008

EVALUATED PRODUCT: Gemini Trusted Network Processor (GTNP)

VENDOR: Gemini Computers, Incorporated

VERSIONS: GTNP Version 1.01, consisting of: (a) GEMSOS Security Kernel Version 2.01, configurations 0007, 0029, 0031, 0032, 0107, 0126, 0127, 0128, or 0129, (b) GEMSOS Network Processor System Parent Version 1.00e. (c) GEMSOS Kernel Gate Library Version 1.03. (d) GEMSOS Multilevel Subject Intersegment Linkage Tool Version 1.00b. Running on either an evaluated Gemini Trusted Base or an evaluated Gemini PC Workstation Kit for selected PC compatibles.

EVALUATION DATE: 06 September 1994

OVERALL EVALUATION CLASS: A1 Mandatory-Only Network Component

PRODUCT DESCRIPTION:

The Gemini Trusted Network Processor (GTNP) provides a Mandatory Network Trusted Computing Base (M-NTCB) for network components that implement a Mandatory Access Control (MAC) policy. In addition to providing multilevel security, the GTNP provides Data Encryption Standard (DES) encryption and concurrent processing. The GTNP is designed to support integration without her technologies and products to build a variety of secure network interconnection and secure data-sharing components for multilevel secure (MLS) and/or multiple security level (MSL) heterogeneous distributed information systems. In these systems, the GTNP provides the trusted underlying foundation upon which applications and protocols are built. Taking an open-architecture approach, users of the GTNP are not restricted to a single application or suite of protocols; rather, applications and protocols may be developed to run on top of the structured base provided by the GTNP to support the specific network requirements or network component composition, without affecting the M-NTCB.

The GTNP is based on the Gemini Multiprocessing Secure Operating System(GEMSOS) Security Kernel (Kernel). The Kernel is a mandatory security reference monitor that enforces a lattice-based MAC policy for both secrecy (confidentiality) based on the Bell-LaPadula model, and integrity based on the Biba model. Support is provided for up to 16 secrecy levels, 64 secrecy categories, 16 integrity levels, and 32 integrity categories. The Kernel implements real time, priority-based scheduling to provide multiprogramming and multiprocessing to support concurrent computing including parallel and pipeline processing.

The GTNP uses DES encryption and cryptographic checksum mechanisms, together with a trusted key management algorithm and other controls to implement trusted distribution. It insures that critical software and hardware are controlled with a high level of assurance throughout their life-cycle.

The GTNP hardware includes a tightly coupled multiprocessing architecture that supports up to eight Intel 80x86 processor boards (a mixture of i486,i386, and 80286 processors), memory boards, and device interface boards on the IEEE standard 796

system bus, Multibus I. The PC bus supports single processor GTNP configurations. All evaluated configurations utilize the Gemini System Controller board, which provides the hardware DES encryption device and bus-arbitration circuitry.

The GTNP supports network interfaces for local area networks using Ethernet and RS-232, and X.25 wide area networks using High-Level Data Link Control (HDLC) protocol; a preallocated address interface (Multibus I); and a virtual machine monitor interface. GTNP Version 1.01 is designed to support single-level network protocols outside the TCB without affecting the evaluation rating of the GTNP.

The GTNP software architecture is implemented on the 80x86 multi-state machine consisting of four hierarchical hardware enforced privilege levels. The Kernel is in the highest privileged level (PL). The GTNP uses the remaining three privilege levels (PL1, PL2, PL3) to implement eight hierarchical rings that can be used to separate processes into different domains. The hierarchical architecture can be used to implement other Network Trusted Computing Base (NTCB) components defined in the TNI, enforcing different security and supporting policies.

Trusted GTNP software is implemented within the lower 5 (more privileged) rings and the Kernel. Applications software is implemented in the higher 3 (less privileged) rings to facilitate effective evaluation of new applications and minimize re-evaluation of the GTNP.

The GTNP supports two types of composite structures: the first is based on the NTCB paradigm of the TNI; the second is based on the TCB Subset paradigm of the TDI. Using these composite structures, enforcement of the overall network security policy may be allocated to the various NTCB components or TCB subsets, with the MAC policy enforcement allocated to the GTNP (and, if necessary, other M-components). Other policies can then be enforced by proper integration of other products with the GTNP.

Within the NTCB paradigm, a secure distributed system with a coherent Network Security Architecture and Design would be composed of multi-vendor network components which can be evaluated in one of two views: the Interconnected Accredited AIS view or the single Trusted System view. The GTNP has been used as the Mandatory Component together with NTCB components provided by other products for trusted security guards, firewalls, access controllers and key distribution centers applications.

Within the TCB Subset paradigm, the overall system TCB would be composed of a number of separately evaluated TCB subsets. The GTNP's hierarchical ring abstraction would be used to provide a layered foundation in which the system TCB is composed of separate trusted software components with distinct domains, i.e, each TCB subset occupies a different ring.

The GEMSOS Security Kernel has been shipped as a commercial product since 1985.

EVALUATION SUMMARY:

The security protection provided by the Gemini Trusted Network Processor, configured according to the most secure manner described in the Trusted Facility Manual, has been evaluated by the National Computer Security Center (NCSC)

against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria [DOD 5200.28-STD] dated December 1985, as interpreted by the Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria [NCSC-TG-005, Version-1], dated 31 July 1987. The GTNP has been evaluated against Appendix A of the Trusted Network Interpretation.

The National Security Agency (NSA) evaluation team has determined that the highest class at which the Gemini Trusted Network Processor satisfies all of the specified requirements of the Criteria as interpreted by the Network Interpretation is as an A1 Mandatory-Only Network Component. As a result, the GTNP can potentially be incorporated into a network system that can meet the Trusted Network Interpretation (of the Trusted Computer System Evaluation Criteria) (TNI) part I requirements for class A1 and several of the TNI part II requirements.

A system that has been rated as being an A division system is characterized by the use of formal security verification methods to assure that the controls provided by the system can effectively protect classified or other sensitive information stored or processed by the system. The system architecture is that of a minimized security reference monitor. Extensive documentation is required to demonstrate that the Trusted Computing Base (TCB)* meets the security requirements in all aspects of design, development, and implementation.

M-Components are components that provide network support of the Mandatory Access Control (MAC) Policy as specified in the TNI. M-Components do not include the mechanisms necessary to completely support any of the other network policies (Discretionary Access Control, Identification and Authentication, and Audit) as defined in the interpretation.

Gemini Computers, Incorporated is participating in the Ratings Maintenance Phase (RAMP) Program for the Gemini Trusted Network Processor. Future changes to the evaluated system will continue to be reviewed via RAMP so as to maintain the rating of the system.

For a complete description of how the Gemini Trusted Network Processor satisfies each requirement of the Criteria, see Final Evaluation Report, Gemini Trusted Network Processor (Report No. CSC-EPL-94/008). The report should also be consulted for an exact list of the evaluated hardware components.

* In the case of network component evaluations, this demonstration is for the Network TCB (NTCB) component partition.

Serial No. CSC-EPL-93/008

EVALUATED PRODUCT: HP-UX BLS

VENDOR: Hewlett Packard

VERSION: Release 8.04

EVALUATION DATE: 21 September 1993

OVERALL EVALUATION CLASS: B1

PRODUCT DESCRIPTION:

Hewlett Packard's HP-UX BLS (B Level Security) is HP's version of a Unix operating system which is designed to meet the DoD Trusted Computer System Evaluation Criteria for a B1 class rating. The vendor claims that HP-UX BLS is compatible with the System V Interface Definition 2 and IEEE POSIX 1003.1 and 1003.2 standards. HP-UX BLS also includes important features from Berkeley Software Distribution 4.3, and runs on evaluated models in the HP9000/S800 family of computers.

HP incorporated a standard trusted system technology developed by SecureWare, an independent software firm, into HP-UX, HP's standards-based, multi-user, multi-tasking UNIX computing environment. HP-UX BLS is designed to provide B1 level security in a multi-user environment. The essence of HP-UX BLS is multi-level security characterized by the concept of subject/object sensitivity labeling in conjunction with a Mandatory Access Control (MAC) policy. The MAC policy enables the assignment of initial clearance levels (or labels) for users, files, devices, and interprocess communication. The MAC policy also provides control of distribution of information protected by the system to only those users who have been authorized for the information. The MAC policy is derived from the Bell-La Padula model and conforms to Department of Defense policy for mandatory access control. A large number of classifications and compartments are supported. Within the access constraints set by the MAC policy, users can at their discretion authorize or restrict access to files they own. This is accomplished by way of an implementation of Discretionary Access Control policy through Access Control Lists (ACLs) used in combination with traditional UNIX access controls specified through protection bits. Users can, in a controlled manner, assume the user or group identity of another user or group in order to perform tasks that are restricted to the assumed user or group.

Other enhancements include: a password management mechanism that is designed to meet the objectives and recommendations of the DoD Password Management Guideline, CSC-STD-002-85; several security databases to protect and control passwords, terminal access, system files, system defaults, and device assignment; the concept of restricted privileges that ensures a program is granted only enough privilege to perform its functions, and users have only those privileges sufficient to perform their assigned tasks; an import/export facility that ensures that data can be securely imported and exported to and from a multi-level secure environment; the concept of multi-level directories that allows processes with different sensitivity labels to access files public directories securely;

and an enhanced auditing subsystem that logs security relevant events to ensure user accountability.

EVALUATION SUMMARY:

The security protection provided by HP-UX BLS, configured according to the most secure manner described in the Trusted Facility Manual, has been evaluated by the National Security Agency (NSA) against requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria [DOD 5200.28-STD] dated December 1985.

The evaluation team has determined that the highest class at which HP-UX BLS satisfies all the specified requirements of the Criteria is class B1. In addition, HP-UX BLS satisfies the functionality of the B3 requirement for DAC and the B2 requirement for Trusted Facility Management.

Subject: IBM MVS/ESA EPL Entry SERIAL NO. CSC-EPL-SUM 90/002

EVALUATED PRODUCT: Multiple Virtual Storage / System Product (MVS/SP)
Job Entry Subsystem 2 (JES2)
Job Entry Subsystem 3 (JES3)
Data Facility Product (DFP)
Resource Access Control Facility (RACF)
Time Sharing Option / Extensions (TSO/E)
Advanced Communications Function /
Virtual Telecommunications Access Method
(ACF/VTAM)*
Print Services Facility (PSF)
Enterprise Systems Architecture/370 (ESA/370)*
(collectively referred to as MVS/ESA*)

VENDOR: International Business Machines Corporation

VERSION EVALUATED:
MVS/SP Version 3 Release 1.3
JES2 Version 3 Release 1.3
JES3 Version 3 Release 1.3
DFP Version 3 Release 1.1
RACF Version 1 Release 9
TSO/E Version 2 Release 1.1
ACF/VTAM ESA Version 3 Release 3
PSF Version 1 Release 3

EVALUATION DATE: 17 September 1990

OVERALL EVALUATION CLASS: B1

PRODUCT DESCRIPTION:

MVS/SP is IBM's operating system for its computers that offer the Enterprise Systems Architecture (ESA/370). The system provides generalized facilities that support a wide variety of usages including concurrent execution of multi-user time-sharing, batch, and real-time applications.

RACF is IBM's strategic facility for providing security services and support to MVS/SP. RACF provides numerous functions and features that greatly enhance an installation's control over its resources. RACF's flexibility and functionality supply a common base for security within many IBM products.MVS/SP with RACF make available privilege and protection mechanisms to limit user access to system-controlled structures in physical storage, system-structured volumes and files, and certain devices. The evaluated software encompasses all other products listed above supplying MVS/SP with a wide functionality. Furthermore, several MVS/ESA systems may be operated together within an MVS/ESA JES complex while retaining the overall rating. Even though MVS/ESA has all the features necessary for networking, the B1 rating applies to only those MVS/ESA systems utilized as stand-alone systems.

MVS/ESA uses resource access control lists to provide discretionary access controls and maintains a security label for each subject and object by which mandatory access control decisions are made. Additionally, MVS/ESA provides user identification and authentication through user IDs and passwords, and individual accountability through its auditing capability. The ESA/370 architecture specifies several protection mechanisms. In general, user programs execute in the problem state while the system programs run in the supervisor state. User separation is achieved with an extensive memory and address space management. System programs are further isolated by means of protection keys.

The evaluated software is supported by IBM processors supporting ESA/370.This product line ranges from mid-range 4381 computers to 3090 main frames with six central processors and six vector facilities. In addition, fifteen models of the 3090 computers may be operated in certain partitioned configurations while maintaining the security of each system and, hence, the awarded rating.

EVALUATION SUMMARY:

The security protection provided by MVS/ESA, configured according to the most secure manner described in the Trusted Facility Manual, has been evaluated by the National Computer Security Center (NCSC) against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria [DOD 5200.28-STD] dated December 1985.

The NCSC evaluation team has determined that the highest class at which MVS/ESA satisfies all the specified requirements of the Criteria is class B1. Due to IBM's decision not to participate in the Ratings Maintenance process, the NCSC is unable to evaluate future changes to the system.

The rating given to the evaluated system (viz., B1) is the highest level of the Criteria at which the system satisfies all the specified requirements. For a complete description of how MVS/ESA satisfies each requirement of the Criteria, see Final Evaluation Report, International Business Machines Corporation MVS/ESA (Report CSC-EPL-90/002). In addition, the Report should also be consulted for the complete lists of evaluated hardware and software components as well as all the necessary PTF numbers.

* MVS/ESA, ACF/VTAM, and ESA/370 are registered trademarks of the IBM Corporation.

Subject: EPL Data Bases Serial No. CSC-EP-93/004

EVALUATED PRODUCT: INFORMIX-OnLine/Secure

VENDOR: Informix Software, Inc.

VERSION EVALUATED: Release 4.1

EVALUATION DATE: 21 March 1994

OPERATING SYSTEM PLATFORM:

AT&T System V/MLS 1.2.0 running System V 3.1.1
Harris CX/SX Release 6.1.1
Harris CX/SX with LAN/SX Release 6.1.1
Hewlett Packard HP-UX BLS Release 8.04

OVERALL EVALUATION CLASS: C2

PRODUCT DESCRIPTION:

INFORMIX-OnLine/Secure installed in its C2 configuration is a relational database management system (RDBMS) for multi-user, multi-tasking UNIX platforms and is based on the commercial INFORMIX-OnLine database server. In the evaluated configuration, OnLine/Secure executes as a single-level, trusted application on one of the evaluated operating systems listed above. All of the operating systems listed were evaluated at B1, but can be configured to process information at multiple sensitivity levels, one of which is to protect the integrity of the TCB and the others are for users. Note that this is not required with the HP-UX BLS product but is a recommended procedure. The OnLine/Secure component of the TCB provides an SQL interface that meets the requirements of the U.S. National Institute of Standards and Technology (NIST) for certification of the ANSI SQL89 Level 2 (FIPS 127-1) standard. Applications and application development tools for OnLine/Secure maintain compatibility with the commercial OnLine product, INFORMIX-OnLine. By integrating secure features with the commercial product, customers get features such as high performance, fault tolerance, and multimedia capability while meeting their demands for security and trust.

OnLine/Secure users can authorize or restrict access to RDBMS objects they own on the basis of "need to know." This Discretionary Access Control (DAC) policy is implemented by allowing owners of RDBMS objects to grant various privileges on those objects, allowing them to be shared with other users. This DAC policy is completely disjoint from the DAC policy enforced by the operating system. Resources subject to the DAC policy include the RDBMS abstractions of databases and tables. Appropriate database privilege must be held by users who want to access tables within a specific database, in addition to privilege to the specific target table. In addition, compliance with the object reuse requirement is accomplished by not allowing a user to read an object before it has been written into.

OnLine/Secure uses the identification and authentication of the operating system to implement its accountability policy. OnLine/Secure enhances operating system audit logs with RDBMS auditing records that record RDBMS security relevant events such as database/table access and manipulation and RDBMS administrator actions. The operating system's audit subsystem is used to maintain these audit records.

OnLine/Secure supports three administrative roles to facilitate administration of the system and to control the use of restricted security commands. One role is the Database System Security Officer, whose primary function is to maintain the security attributes of all the RDBMS users and objects. Another role is the Database System Administrator, whose responsibility is to perform non-security critical system tasks such as configuration and initialization of the RDBMS system and performing general maintenance when required. The third role is the Audit Analysis Officer, whose primary goal is to review and analyze the OnLine/Secure audit data.

Other features offered by OnLine/Secure include:

* an Import/Export utility that ensures that data can be securely imported and exported to and from another Informix secure environment

* a trusted front-end for use by the RDBMS security officer.

EVALUATION SUMMARY:

The INFORMIX-OnLine/Secure C2 composite TCB can be configured to satisfy all the specified requirements in the Trusted Database Interpretation of the Trusted Computer System Evaluation Criteria, dated April 1991. The Trusted Facility Management documents, the INFORMIX-OnLine/Secure Administrator's Guide and the operating systems' trusted management documents, describe how to initialize the system into a C2 mode to support the above conclusion. The NSA evaluation team has determined that the highest class at which INFORMIX-Online/Secure system executing on one of the operating systems listed above satisfies every requirement is C2. For a complete description of how the Informix portion of the composite TCB is designed to satisfy each requirement of the TDI, see Final Evaluation Report CSC-EPL-93/004.

EVALUATED PRODUCT: INFORMIX-OnLine/Secure Release 5.0

VENDOR: Informix Software, Inc.

VERSION EVALUATED: Release 5.0

RAMP DATE: November 15, 1994

OPERATING SYSTEM PLATFORM: Harris CX/SX Release 6.1.1, Harris CX/SX with LAN/SX Release 6.1.1

OVERALL EVALUATION CLASS: C2

PRODUCT DESCRIPTION:

INFORMIX-OnLine/Secure installed in its C2 configuration is a relational database management system (I the evaluated operating systems listed above. All of the operating systems listed were evaluated at B1, and can be configured to process information at multiple sensitivity levels. On the Harris operating system, one sensitivity level is used to protect the integrity of the TCB and the others are for users.

The OnLine/Secure also provides an SQL interface that meets the requirements of the U.S. National Institu OnLine product, INFORMIX-OnLine. By integrating secure features into the commercial product, customers get advanced COTS features such as high performance, fault tolerance, and multimedia capability while also meeting their demands for security and trust.

OnLine/Secure supports three administrative roles to facilitate administration of the system and to control t Administrator, whose responsibility it is to perform non-security related but critical system tasks such as configuration and initialization of the RDBMS system and performing general maintenance when required. The third role is the Audit Analysis Officer, whose primary goal is to review and analyze the OnLine/Secure audit data.

OnLine/Secure users can authorize or restrict access to RDBMS objects they own on the basis of "need to l completely separate from the DAC policy enforced by the operating system, yet it complements the OS DAC policy by applying access attributes specific to RDBMS objects. Resources subject to the RDBMS DAC policy include the RDBMS abstractions of databases and tables. Appropriate database privileges must be held by users who want to access tables within a specific database, in addition to privilege to the specific target table.

OnLine/Secure uses the operating system's identification and authentication routines to implement its accou administrator actions. The operating system's audit subsystem is used to store these audit records. OnLine/Secure also provides administrative audit tools to extract and analyze the recorded security relevant events. These audit records can also be loaded by the RDBMS administrator into a database for more detailed analysis. In addition, compliance with the object reuse requirement is accomplished by not allowing a user to read an object before it has been written into.

Other features offered by OnLine/Secure include:

* an Import/Export utility that ensures that data can be securely imported and exported to and from another Informix multi-level secure environment

* a trusted front-end for use by the RDBMS security officer.

* stored procedures for users to optimize frequently used operations.

* discrete privileges to allow trusted users to perform special database manipulation functions such as downgrading the security level of the database session.

* two-tier auditing for the Audit Analysis Officer to audit finer granularity of auditable events.

* referential integrity for users to enforce data integrity across tables.

* check constraints for users to enforce user-defined range of valid data values.

* default column value for users to allow a column without a value to default to some user-predefined value.

* additional statistical functions (standard deviation, median and variance) for users to compute numeric data.

EVALUATION SUMMARY:

The INFORMIX-OnLine/Secure C2 composite TCB can be configured to satisfy all specified requirements operating systems' trusted management documents, describe how to initialize the system in the C2 mode to support the above conclusion.

The NSA evaluation team has determined that the highest class at which the INFORMIX-OnLine/Secure s description of how the Informix portion of the composite TCB is designed to satisfy each requirement of the TDI, see Final Evaluation Report TBD. See also CSC-EP-94/005.

Subject: EPL Subsystems Serial No.CSC-EPL-91/001

EVALUATED PRODUCT: LOCKIT Professional 2.10

VENDOR: Security Microsystems, Inc.

VERSION: LOCKIT Professional 2.10

OVERALL EVALUATION CLASS: I&A / D
DAC / D
AUD / D
OR / D

EVALUATION DATE: 27 March 1991

PRODUCT DESCRIPTION:

LOCKIT Professional 2.10 is a microcomputer hardware and software package which operates on an IBM PC, PC/XT, PC/AT, or 100% BIOS compatible microcomputer under MS-DOS or PC-DOS. The product is a combination of a hardware board and a software package which allows many users to share a system, one at a time. The package provides a friendly user interface, a manual for the System Administrator, and a User's manual.

EVALUATION SUMMARY:

The Trusted Product and Network Security Evaluations Division of the National Security Agency (NSA) has evaluated the security protection provided by LOCKIT Professional 2.10. The security features for Identification and Authentication, Discretionary Access Control, Audit, and Object Reuse were evaluated against the Computer Security Subsystems Interpretation (CSSI) of the Trusted Computer Security Evaluation Criteria (TCSEC).

LOCKIT Professional 2.10 is a subsystem which provides Identification and Authentication, Discretionary Access Control, Object Reuse, and Auditing. The user is confined within a menu driven environment which must not be exited if security is to be maintained. Identification and Authentication is accomplished within a separate domain before MS/PC-DOS is brought up.

Discretionary access control is obtained by defining a limited access area for each user and by providing access to that area only through that user's menu. Object reuse functionality for both memory resident objects and disk resident objects can be set so that it is automatically invoked. Auditing capabilities arevery limited. There are limited checks to determine if any part of LOCKIT Professional 2.10 was tampered with.

LOCKIT Professional 2.10 receives a D rating in auditing because it does not meet all of the functional requirements for a higher rating. In addition to meeting the functionality requirements defined in the CSSI, subsystems must also meet the assurance and documentation requirements. LOCKIT Professional failed to satisfy the assurance and documentation requirements, and therefore receives a composite rating of D for the Identification and Authentication, Object Reuse, and Discretionary Access Control features.

For a complete description of how LOCKIT Professional satisfies each requirement of the CSSI, see Final Evaluation Report,Security Microsystems, Inc. Lockit Professional (Report No. CSC-EPL-91/001).

Serial No. CSC-EPL-91/005

EVALUATED PRODUCT: MLS LAN Secure Network Server System

VENDOR: Boeing Space and Defense Group

EVALUATION DATE: 28 August 1991

OVERALL EVALUATION CLASS: A1 MI Network Component

PRODUCT DESCRIPTION:

The Boeing Multi-level Secure Local Area Network (MLS LAN) Secure Network Server System is a data communications network component which can support the simultaneous transmission of digital data and analog video within a local area. The MLS LAN Secure Network Server System provides communications between attached devices (e.g., hosts, terminals, and analog video equipment) which may be operating at different sensitivity levels. MLS LAN Secure Network Server System is comprised of multiple Secure Network Servers (SNSs) connected by a transmission medium (Ethernet and optionally, a fiber-optic trunk for video transmission).

The MLS LAN Secure Network Server System provides user and network services including:

- Host-to-host reliable communications with either TELNET or TCP.

- Host-to-host datagram service with UDP.

- Network terminal-to-host TELNET communications.

- User-to-user terminal message service.

- Video circuit-switched services.

An SNS is a network access device with embedded upper-level DOD protocols including IP, TCP, TELNET and UDP. SNSs support terminal, serial host, multiplexed host and video subscriber devices, as well as Network Management Workstation and Audit Server interfaces. An SNS is modularly expandable to support various configurations of subscriber devices.

Terminals are attached to an SNS terminal device interface card which performs user identification and authentication, access control and auditing functions. A terminal user may connect to hosts on the network according to mandatory and discretionary access controls. Up to eight seperate TELNET sessions may be active simultaneously from one terminal, potentially operating at different sensitivity levels.An inter-terminal message (ITM) service allows network terminal users to exchange short messages. Authorized terminal users may also request video services, which use video cameras and video cassette recorders as input and output equipment.

Hosts are attached to an SNS through either a serial device interface card or a host device interface card. The protocol between a host interface connected host and an SNS supports multiple logical channels over the single physical interface, with each channel capable of

supporting UDP, TCP and TELNET communication services. TELNET is the only service offered to a host connected to a serial device interface.

The MLS LAN Secure Network Server System uses a distributed network management approach, with the SNSs providing local management support. Additionally, SNSs provide a network management workstation interface to a centralized Network Management Workstation and Audit Server that,when added to the MLS LAN Secure Network Server System, provides system-level monitoring and control.

EVALUATION SUMMARY:

The security protection provided by MLS LAN Secure Network Server System has been evaluated by the National Security Agency (NSA). The security features of MLS LAN Secure Network Server System were tested against the requirements specified by the ``Department of Defense Trusted Network Interpretation," (TNI) dated July 1987. The NSA evaluation team has determined that the highest class at which MLS LAN Secure Network Server System satisfied the requirements set forth in the TNI is A1 MI network component.

For a complete description of how MLS LAN Secure Network Server System satisfies each requirement of the TNI as an A1 MI network component,see Final Evaluation Report, Boeing Space and Defense Group, MLS LAN Secure Network Server System (Report No. CSC-EPL-91/005).

Serial No. CSC-EPL-94/006

EVALUATED PRODUCT: MLS LAN

VENDOR: Boeing

EVALUATED VERSION: 2.1

EVALUATION DATE: 15 August 1994

OVERALL EVALUATION CLASS: A1 MDIA Network Component

PRODUCT DESCRIPTION:

Boeing's MLS LAN is an A1 MDIA component that is capable of interconnecting hosts, terminals, and IP networks at different security levels. In addition to the data communications features, it can simultaneously support the transmission of analog circuit-switched data,such as video. As an MDIA component, the MLS LAN enforces Mandatory and Discretionary Access Control policies on communications between attached devices (e.g., hosts, terminals, and analog circuit-switched equipment); provides auditing of security-relevant events; it is also capable of providing Identification and Authentication services for user connections that have one or both end points within the MLS LAN partition.

The basic unit of the MLS LAN is the Secure Network Server (SNS). An SNS is modularly expandable to support various configurations of subscriber devices. The basic SNS includes a chassis with system memory, an SNS processor (SNSP), and an IEEE 802.3 trunk interface. To achieve a desired level of functionality, subscriber device interface cards are added to the SNS. Two versions of the SNS are available. SNS-1000s are based on the 286 Intel processor; SNS-2000s are based on the 386 Intel processor. The two versions are inter operable, but have different capabilities.

The MLS LAN is made up of one or more Secure Network Servers (SNSs) connected by an Ethernet trunk. This trunk cannot be used to attach subscriber devices. One SNS-2000 on the trunk must include the evaluated network management software and must have network management terminals attached to it. Each SNS can be expanded to provide additional RS232 and IEEE 802.3 (Ethernet) interfaces for attaching terminals and computers. The following services are provided at these interfaces:

* Serial Multiplexing and "terminal switch" Service, which provides for Terminal to Host and Host to Host serial connections, is a serial port rotary service that allows a host with multiple serial interfaces to have a single user-visible host name.

* Serial to TELNET gateway service allows users on RS232 devices (such as terminals or serially-attached hosts) to connect to a destination host using the TELNET protocol. This service will also provide authentication information to the destination host in the DNSIX format if the host is configured to utilize this information.

* Write-up Connection Service allows high level ethernet-attached hosts to accept connections from lower-level terminal and host users.The write-up connection service requires a

host that understands both the Internet Protocol (IP) and the World-Wide Military Command and Control System (WWMCCS) protocols.

* IP Datagram Forwarding Service provides static routing between two ethernet-attached IP devices. These devices may both be IP hosts, IP networks, or a combination of the two.

* Inter terminal message service can be used to send messages between two users signed on at terminal interfaces.

* An Audit Server interface allows the connection of an optional, external, audit server. The external server does not receive any information that is not available through the internal network management software, but the external server may be used to search and sort the audit records in ways that the internal software doesn't allow.

* Analog circuit-switched services can be used to connect analog transmitters, such as video cassette players or video cameras, to analog receivers, such as television monitors. Analog circuit-switched services are only available on the SNS-1000.

PRODUCT STATUS:

The MLS LAN has been developed by Boeing's Defense and Space Group.The MLS LAN is an upgraded and enhanced version of Boeing's MLS LANSecure Network Server System that earned an A1 MI component rating.The transition to this product included the addition of a network management node as well as enhancements and restructuring to hardware and software. The MLS LAN is currently available.

SECURITY EVALUATION STATUS:

The formal evaluation was completed in July of 1994. The security protection provided by the MLS LAN has been evaluated by the National Security Agency (NSA) against the requirements specified by the Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria (TNI), 31 July 1987, NCSC-TG-005, Version 1.

The NSA evaluation team has determined that the highest class for which the MLS LAN satisfies all the specified requirements of the TNI is class A1 as an MDIA network component. A class A1 MDIA network component minimally fulfills all the requirements as stated in Appendix A of the TNI for a class A1 Mandatory Access Control component, a class C2+Discretionary Access Control component, a class C2 Identification & Authentication component, and a class C2+ Audit component.

The MLS LAN covert channel analysis is applicable only to the MLS LAN NTCB partition. While it is possible to include an evaluated network M-component such as the MLS LAN as part of a network system incorporating other M-components (such as multilevel hosts), this may introduce new covert channels or penetration scenarios that were not evident from the evaluation of either component by itself. A complete network system must always be evaluated as a whole to ensure that the components together enforce the overall policy.

In addition to the network component rating, the NSA evaluation team has determined that the MLS LAN provides some of the security services described in Part II of the TNI. The NSA no longer assigns specific ratings to these services, but discusses them in the Final Evaluation Report

(FER) of the product. The Part II services that are offered by the MLS LAN are Authentication, Communications Field Integrity, Continuity of Operations, Network Management, and Selective Routing.

For a more in depth description of the MLS LAN refer to the Final Evaluation Report, Boeing Corporation, MLS LAN (Report No. CSC-EPL-94/006).

Serial No.: CSC-EPL-93/002

EVALUATED PRODUCT: OpenVMS VAX

VENDOR: Digital Equipment Corporation

VERSION: 6.0 with VAXSMUP03_060

EVALUATION DATE: 30 June 1994

[Note: The original evaluation date was 31 August 1993.

OVERALL EVALUATION CLASS: C2

PRODUCT DESCRIPTION:

Digital Equipment Corporation's OpenVMS VAX Version 6.0 with VAXSMUP03_060is a general purpose multi-user operating system running on Digital's Virtual Address Extension (VAX) processors. The VAX processor hardware supports OpenVMS protection mechanisms by providing four hierarchical hardware access modes and memory page protection based on those modes. In addition, the VAX hardware architecture provides support for process isolation through virtual memory management and process context switching. The evaluated configuration includes both stand alone VAX systems and VAX clusters configured with a common environment, where a single user authorization database is used by all of the nodes of the cluster to enforce a unified security policy.

Basic discretionary access controls are provided by user categories (system, owner, group, and world). In addition, access control lists are supported that contain identifiers and the authorized access for the identifier. A user may be associated with a number of different identifiers, providing a flexible mechanism for grouping access permissions based on identifiers.

Security administration features provided by OpenVMS include support for user registration with password management options and restricted user environments, audit collection and analysis, and delegation of administrative authority using OpenVMS system privileges. Object reuse features include memory initialization, disk and tape erasure options, and printer reset sequences.

Features of OpenVMS that provide security functionality extending beyond the C2 requirements include address space isolation, trusted path for login, and access control lists.

PRODUCT STATUS:

OpenVMS is developed, marketed, and supported by Digital Equipment Corporation. OpenVMS VAX Version 6.0 with VAXSMUP03_060 was released in February of 1994. Digital is participating in the NCSC Rating Maintenance Program (RAMP); future releases of OpenVMS may appear on the EPL as a result of a RAMP action.

EVALUATION SUMMARY:

The security protection provided by OpenVMS VAX Version 6.0 with VAXSMUP03_060 has been evaluated by the National Computer Security Center(NCSC) against the requirements specified by the "Department of Defense Trusted Computer System Evaluation Criteria" [DOD 5200.28-STD] (the Criteria) dated December 1985.The NCSC evaluation team has determined that the highest class at which OpenVMS VAX Version 6.0 with VAXSMUP03_060 satisfies all the specified requirements of the Criteria is class C2. For a complete description of how OpenVMS satisfies each requirement of the Criteria, refer to the Final Evaluation Report, OpenVMS VAX and SEVMS VAX Version 6.0 (Report NCSC-EPL-93/xxx). In addition, the final evaluation report should be consulted for the complete list of evaluated hardware and software, as well as constraints on the hardware and software configurations that have been evaluated.

The figure below indicates the requirements and corresponding level that OpenVMS VAX Version 6.0 with VAXSMUP03_060 satisfies.

ENVIRONMENTAL STRENGTHS:

OpenVMS provides a flexible discretionary access control mechanism that can be used to define complex controls for sharing access. Account restrictions can be specified by an administrator to provide flexible controls on the environment and system resources accessible to individual users.

When used within the common VAX cluster environment, OpenVMS provides a distributed computing environment with a uniform security policy. OpenVMS also supports security features not required by the TCSEC, including break-in detection mechanisms, password management options, and data access control using application subsystems.

* OpenVMS, VAX, and VAX cluster are registered trademarks of Digital Equipment Corporation.

Serial: CSC-EPL-89/004.D

RATING MAI**NTENANCE PRODUCT**: OS 1100/2200 Release SB4R7

ORIGINAL EVALUATED PRODUCT: OS 1100 Security Release I

VENDOR: Unisys Corporation

RATING MAINTENANCE DATE: 20 April 1994

OVERALL EVALUATION CLASS: B1

EVALUATION SUMMARY:

Unisys Corporation has maintained the B1 rating of its OS1100/2200 product through participation in RAMP. For more information on this product see the new Final Evaluation Report Addendum addressing OS 1100/2200 Release SB4R7.

PRODUCT DESCRIPTION:

OS 1100/2200 Release SB4R7 is a general purpose, multi-processing operating system running on Unisys 1100/90, 2200/100, 2200/200,2200/400, 2200/600, 2200/600ES and 2200/900 hardware. These models share a similar architecture which employs a multi-state protection mechanism along with hardware memory protection. OS 1100/2200 is structured to take advantage of these architectural features. For example, it supports multiple processes (activities), each running with a private virtual address space and capable of sharing protected subsystems (common memory banks).OS 1100/2200 Release SB4R7 supports batch, time-sharing(demand), and transaction processing (TIP) modes. The trusted computing base (TCB) of OS 1100/2200 Release SB4R7 consists of specific releases of the following components: Executive, CMS1100, TELCON, SOLAR, PC Console, COMUS, FAS, IRU, LA, UDSC, MCB, PERCON, SIMAN, SSP/SCF, TLABEL, and DPREP1100. Communications are provided by Distributed Communications Processors (DCPs) operating as front end processors under control to CMS 1100 and TELCON. The OS 1100/2200 Executive is the base component and a prerequisite for the other components. The TCB enforces a mandatory and discretionary security policy, performs user identification and authentication, clears residue, generates audit trail and accounting records, and provides a base upon which to build secure application programs.

OS 1100/2200 Release SB4R7 provides isolation of the OS 1100/2200 Executive through the use of hardware protection mechanisms. Access to OS 1100 subsystems (shared memory banks) is protected with controlled access to entry points (gates). If access is permitted to the entry point, the system switches the security attributes of the process (activity) to those specified for the subsystem. Activity isolation is achieved by using a hardware and software architecture which includes a per-activity virtual address space, per-activity stacks, and architecturally defined activity state changes.

OS 1100/2200 Release SB4R7 provides a mandatory access control policy consistent with the Bell-LaPadula model. Mandatory access control is based on labeling which supports up to 64 hierarchical levels and 30 categories. An administrator can attach symbolic names to each

level and each category. Additionally, each category may be securely re-defined by an administrator. OS 1100/2200 requires that all subjects and objects have a mandatory label and ensures that all accesses to objects conform to the security policy.

Discretionary access control provided by OS 1100/2200 Release SB4R7 is based on access lists which may be private(default), public, or semi-private (access control record attached). Access control records specify by whom, when, and how the object may be accessed. OS 1100/2200 not only provides discretionary access controls available for individual users, access may be controlled at a group level as well.

OS 1100/2200 Release SB4R7 provides clearing of residue (object reuse) in registers, main storage, and mass storage.

Identification and authentication of batch, demand, and TIP users is accomplished by presenting a userid and password to the TCB's Login facility. Identification and authentication information is stored in a protected database in the OS 1100/2200 file system.

OS 1100/2200 Release SB4R7 provides an auditing facility to ensure user accountability. All security-relevant events are always audited, not just auditable. This facility includes collection, reduction, backup, and audit data recovery capabilities. The Log Analyzer (LA) provides audit reduction capabilities including security reports, actions of individual users, and references to specific objects or object security levels.

OS 1100/2200 also provides the ability to restrict user privileges to those required to perform their duties. All users (including operators and administrators) are subject to this mechanism. The system supports a Security Administrator role. This administrator is responsible for the overall security of the system. Sub-administrators can also be defined to the system. System operators and administrators are trusted individuals and their interactions with the system are audited.

OS 1100/2200 Release SB4R7 also provides some features beyond those required for a class B1 system. These include B2 trusted path, B3 DAC for groups, and B2 trusted facility management.

PRODUCT ENHANCEMENTS:

This RAMP action introduces the following improved functionality and enhancements:

OS 1100/2200 Release SB4R7 contains no changes to the security policy, features or mechanisms provided by the originally evaluated product. This release is primarily a maintenance release but contains a few features, some performance enhancements, along with maintenance fixes.

The new features of SB4R7 include the final software adapts for the 2200/900 and adapts for future hardware systems. Included in the adapts are internal infrastructure and addressing changes.

A new hardware mainframe (2200/900) and new peripherals are introduced with SB4R7. The new peripherals include the DCP600 Series. Refer to the Final Evaluation Report Addendum addressing OS 1100/200 Release SB4R7 for a current list of available mainframes and peripherals.

Serial: CSC-EPL-94/003

EVALUATED PRODUCT: Oracle 7

VENDOR: Oracle Corporation

RELEASE: 7.0.13.1 with the Procedural Option

DATE: 5 April 1994

OVERALL EVALUATION CLASS: C2

PRODUCT DESCRIPTION:

As the foundation for Oracle's secure cooperative server technology, Oracle7 running on HP-UX BLS is designed to meet international commercial and government security standards. Oracle7 is certified by NIST as 100% compliant for ISO5057/ANSI SQL89 level 2 including the integrity enhancement feature. Oracle7 includes support for stored procedures, triggers, declarative integrity constraints, synonyms, asynchronous replication, and resource limits.

Discretionary access control in Oracle7 is achieved through the use of privileges. The privileges come in two forms: object and system privileges. Object privileges control access to particular database objects. System privileges control use of SQL commands. In order to facilitate privilege administration, Oracle7 privileges can be grouped in roles. Roles are defined groups of privileges that can be granted to users and other roles.

Oracle7 controls object reuse by allocating storage objects for use as part of an Oracle7 table space only after all traces of remnant data are removed.

Oracle7 provides authentication via the identification and authentication mechanism of the underlying operating system.

Oracle7 provides a highly configurable set of auditing capabilities. Oracle7 provides the ability to selectively audit very specific operations by narrowing the scope of the audit to only the desired information, thereby reducing the system resources needed for auditing. Application specific auditing can be implemented using Oracle7 triggers.

Oracle7 provides extensive data integrity features in addition to its security features. Oracle7 uses row-level locking and multi-version read consistency to provide high performance concurrency controls. Declarative integrity constraints and trigger procedures can be used to assure that the data maintained by Oracle7 is constrained by the business rules defined for the database.

EVALUATION SUMMARY:

Oracle7 was evaluated against the "DoD Trusted Computer System Evaluation Criteria", DoD 5200.28-STD, dated December, 1985 as interpreted by the "Trusted Database Interpretation of the

Trusted Computer System Evaluation Criteria", dated April 1991 as a C2 class database management system.

The NSA evaluation team has determined that the highest class at which Oracle7 running on HP-UX BLS satisfies all specified requirements of the Criteria is class C2. For a complete description of how Oracle7 running on HP-UX BLS satisfies each requirement of the TCSEC and TDI, see the Final Evaluation Report, Oracle Corporation Oracle7 and Trusted Oracle7 (Report CSC-EPL-94/003).

Oracle Corporation has satisfied the requirements for participation in the Ratings Maintenance Program (RAMP) and it is anticipated that ports to additional platforms will be evaluated under RAMP.

Serial No. CSC-EPL-94/009

EVALUATED PRODUCT: RAC/M and RAC/M II

VENDOR: Okiok Data Ltd.

VERSION: 3.3 for DOS Windows

EVALUATION DATE: October 17, 1994

OVERALL EVALUATION CLASS: I&A / D2
OR / D2
DAC / D3
AUD / D2

PRODUCT DESCRIPTION:

The Resource Access Control and Management product, or RAC/M, is a product designed to maintain the protection and confidentiality of files and data on 80x86 personal computers (PC's). RAC/M provides user identification an authentication, auditing and access control to computer resources such as serial ports and parallel ports as well as transparent disk access control and encryption. An Application Program Interface is also available to embed security services within an application program. It is available for both Industry Standard Architecture (ISA) and Micro Channel Architecture bus machines (the RAC/M II Version). The evaluation specifically applies to RAC/M.

The Product allows multiple users to share a single PC in a controlled manner by providing for access restrictions. There are no required limits on the type of software which can be run on the PC by a user. RAC/M can be used in two main types of applications: to ensure that only authorized users access the PC; and to ensure that in addition to controlling access to the PC, specific users can be prevented from accessing specific data.

EVALUATION SUMMARY:

RAC/M has been evaluated by the Communications Security Establishment (CSE) in Canada against the Canadian Trusted Computer Product Evaluation Criteria(CTCPEC) and received the following CTCPEC ratings at the T-1 assurance level:CM-2, CR-1, IB-1, IP-1, IS-3, AY-2, WA-2, WI-2, WT-2. The National Security Agency (NSA) has analyzed the findings of the CSE evaluation, and mapped the results of the evaluation to the applicable set of ratings under the Computer Security Subsystem Interpretation of the DoD Trusted Computer Security Evaluation Criteria (CSSI).

A DAC subsystem provides a policy for owners of objects to control access to those object. Access decisions are based on user identifications. A DAC/D3 subsystem must ensure that objects are protected by default, that protection can be enforced to the level of individual users or groups of users, and that denial of access can be enforced to the level of individual users or groups of users. RAC/M users user templates to enforce access control. Each template lists the objects accessible and the access mode permitted, as well as objects to which access is denied. In

RAC/M, the level of protection is at the logical device level, i.e., logical disk drives and logical ports. Untrusted users cannot own these devices; therefore, all permissions are set by the security officer.

An OR subsystem ensures that there are no unauthorized information flows as a result of sharing storage objects between users. Host RAM is cleared by cycling the power between user sessions. RAC/M RAM is cleared by overwriting locations when the contents are no longer required. Logical disk drives are statically created and never reallocated.

An I&A subsystem requires users to identify themselves to it before they do anything on the system. A subsystem rated I&A/D2 must provide a unique identifier and authenticator for each user. Additionally, it must use those items to control access to the protected system, export user identification to the protected system, and must provide an auditing mechanism to log security relevant I&A events. RAC/M provides individual I&A through the use of passwords. For the security officer to logon, a special diskette is required in addition to the correct password for a successful logon. All authentication events are logged by RAC/M.

An Auditing subsystem must e capable of recording all security relevant actions. An AUD/D2 subsystem must be able to integrate into the mechanisms that mediate access and perform user I&A. RAC/M records all security relevant events and interlaces with the I&A mechanisms.

For a complete description of how RAC/M satisfies each requirement, see the Final Evaluation Report, Okiok Data Limited, RAC/M and RAC/M II Version 3.3 for DOS and Windows (CSE Report No. CEPL-002).

Subject: EPL Add on Serial No. CSC-EPL-84/001

EVALUATED PRODUCT: Resource Access Control Facility (RACF)

VENDOR: International Business Machines, Corp.

VERSIONS: RACF Version 1 Release 5

DATE: 23 July 1984

OVERALL EVALUATION CLASS: C1

PRODUCT DESCRIPTION:

RACF is IBM's MVS facility that provides controlled access to system resources. RACF with MVS/370 was the evaluated configuration; however, RACF is also supported under MVS/XA. RACF is designed to limit access to resources by identifying authorized users and protected resources, then controlling users' access to those resources.

RACF also provides the security administrator with the option of default protection on permanent Direct Access Storage Device (DASD) data sets. RACF provides protection for data sets resident on DASD, IBM Mass Storage Systems (MSS) and tape volumes. Access levels of ALTER, CONTROL, UPDATE, READ, and NONE are supported for DASD data sets. Interfaces between RACF and other IBM products, including Information Management System (IMS) and Customer Information Control System (CICS), are supported by IBM.

EVALUATION SUMMARY:

The security protection provided by the IBM Resource Access Control Facility (RACF) Version 1, Release 5 running with the Multiple Virtual Storage/System Product (MVS/SP) 1.3.2 operating system has been evaluated by the Department of Defense Computer Security Center (DoDCSC). The security features of RACF/MVS were evaluated against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria (the Criteria), dated 15 August 1983.

The DoDCSC evaluation team has determined that the highest class at which RACF/MVS satisfies all the specified requirements of the Criteria is class C1. Further, RACF/MVS was found to meet or exceed many of the requirements for class C2.

The overall system integrity level of RACF/MVS is C1. It appears that RACF/MVS can evolve to meet the C2 level of the Criteria, however, RACF/MVS can not meet higher levels of the Criteria without significant modification or reimplementation of a major fraction of MVS and its supporting subsystems.

At the time of the evaluation, MVS was the only operating system that supported RACF Version 1 Release 5. The integrity of RACF is dependent upon the integrity of the MVS system itself.

The rating given to the evaluated system (viz., C1) is the highest level of the Criteria at which the system satisfies all the specified requirements. The "range of feasible use" is intended to convey the overall system integrity level of the system as it is delivered by the vendor and indicates that this system could be used in an environment requiring an evaluation class within this range so long as the missing features are not essential to the operational capability. For a complete description of how RACF/MVS satisfies each requirement of the Criteria, see Final Evaluation

Report, Resource Access Control Facility (RACF), Version 1, Release 5 (Report No. CSC-EPL-84/001).

Serial No.: CSC-EPL-93/003

EVALUATED PRODUCT: SEVMS VAX

VENDOR: Digital Equipment Corporation

VERSION: 6.0 with SEVMS_VAXSMUP03_060

EVALUATION DATE: 30 June 1994

[Note: The original evaluation date was 31 August 1993.

OVERALL EVALUATION CLASS: B1

PRODUCT DESCRIPTION:

Digital Equipment Corporation's SEVMS VAX Version 6.0 with SEVMS_VAXSMUP03_060 is a general purpose multi-user operating system running on Digital's Virtual Address Extension (VAX) processors.The VAX processor hardware supports SEVMS protection mechanisms by providing four hierarchical hardware access modes and memory page protection based on those modes. In addition, the VAX hardware architecture provides support for process isolation through virtual memory management and process context switching. The evaluated configuration includes both stand alone VAX systems and VAX clusters configured with a common environment, where a single user authorization database is used by all of the nodes of the cluster to enforce a unified security policy.

Basic discretionary access controls are provided by user categories (system, owner, group, and world). In addition, access control lists are supported that contain identifiers and the authorized access for the identifier. A user may be associated with a number of different identifiers, providing a flexible mechanism for grouping access permissions based on identifiers.

Mandatory access controls support access mediation based on sensitivity labels associated with both data and users. SEVMS objects that can be shared among users are protected by mandatory access controls.

Security administration features provided by SEVMS include support for user registration with password management options and restricted user environments, audit collection and analysis, and delegation of administrative authority using SEVMS system privileges. Object reuse features include memory initialization, disk and tape erasure options, and printer reset sequences.

Features of SEVMS that provide security functionality extending beyond the B1 requirements include display of subject sensitivity labels, ranges for device labels, trusted path for login, and access control lists.

PRODUCT STATUS:

SEVMS is developed, marketed, and supported by Digital Equipment Corporation. SEVMS VAX Version 6.0 with SEVMS_VAXSMUP03_060 was released in February, 1994. Digital is participating in the NCSC Rating Maintenance Program (RAMP); future releases of SEVMS may appear on the EPL as a result of a RAMP action.

SEVMS is marketed as part of Digital's Security Enhancement Service (SES), a consulting service that includes a security review, security planning, a user orientation, a security manager orientation, and the installation of SEVMS VAX Version 6.0 with SEVMS_VAXSMUP03_060.

EVALUATION SUMMARY:

The security protection provided by SEVMS VAX Version 6.0 with SEVMS_VAXSMUP03_060 has been evaluated by the National Computer Security Center (NCSC) against the requirements specified by the"Department of Defense Trusted Computer System Evaluation Criteria" [DOD 5200.28-STD] (the Criteria) dated December 1985.

The NCSC evaluation team has determined that the highest class at which SEVMS VAX Version 6.0 with SEVMS_VAXSMUP03_060 satisfies all the specified requirements of the Criteria is class B1. For a complete description of how SEVMS satisfies each requirement of the Criteria, refer to the Final Evaluation Report, OpenVMS VAX and SEVMS VAX Version 6.0 with SEVMS_VAXSMUP03_060 (Report NCSC-EPL-93/xxx). In addition, the final evaluation report should be consulted for the complete list of evaluated hardware and software, as well as constraints on the hardware and software configurations that have been evaluated.

The figure below indicates the requirements and corresponding level that SEVMS VAX Version 6.0 with SEVMS_VAXSMUP03_060 satisfies.

ENVIRONMENTAL STRENGTHS:

SEVMS provides a flexible discretionary access control mechanism that can be used to define complex controls for sharing access. Account restrictions can be specified by an administrator to provide flexible controls on the environment and system resources accessible to individual users. The mandatory controls of SEVMS provide access mediation using data sensitivity labels.

When used within the common VAX cluster environment, SEVMS provides a distributed computing environment with a uniform security policy. SEVMS also supports security features not required by the TCSEC, including break-in detection mechanisms, password management options, and data access control using application subsystems.

* SEVMS, SES, VAX, and VAX cluster are registered trademarks of Digital Equipment Corporation.

RAMPED PRODUCT: System V/MLS Release 1.2.0 and 630/MLS Release 1.2.0 running with UNIX System V Release 3.1.1 on the AT&T 3B2/500 and AT&T 3B2/600 minicomputers and the AT&T 630 MTG terminal.

ORIGINAL PRODUCT: System V/MLS version 1.1.2 running with UNIX System V Release 3.1.1 on the AT&T 3B2/500 or AT&T 3B2/600 minicomputers.

VENDOR: American Telephone and Telegraph Co.(AT&T)

RATING MAINTENANCE DATE: 01 September 1992

OVERALL EVALUATION CLASS: B1

EVALUATION SUMMARY:

AT&T has maintained the B1 rating of its System V/MLS product, through participation in RAMP. For more information on this evaluation process and System V/MLS Release 1.2.0, see the new Final Evaluation Report Addendum addressing System V/MLS Release 1.2.0. System V/MLS Release 1.2.0u required no changes to the Final Evaluation Report.

PRODUCT DESCRIPTION:

AT&T's System V/MLS Release 1.2.0 running with UNIX System V Release 3.1.1(hereafter referred to as System V/MLS) is a multi-level secure version of the UNIX System V operating system for the AT&T 3B2/500 and AT&T 3B2/600 minicomputers (both utilizing the WE32100 microprocessor and the WE32101 memory management unit).

System V/MLS is a multi-user, multi-tasking operating system that can support up to 48 concurrent users on a 3B2/500 and up to 64 concurrent users on a 3B2/600. System V/MLS maintains UNIX System V application compatibility, is compatible with the System V Interface Definition (SVID), passes the System V Verification Suite (SVVS), and is source and binary code compatible with existing programs, provided those programs do not require modifications to the System/V MLS Trusted Computing Base (TCB) or violate the system security policy.

In addition to using the traditional protection mechanism of the UNIX operating system to provide discretionary access control, System V/MLS also provides mandatory access control to limit the distribution of information to only those users who have been authorized for it. The mandatory security policy is consistent with the Bell-La Padula model and conforms with DoD policy. System V/MLS provides a flexible labeling scheme that supports up to 255 site selectable hierarchical classification levels and 1024 nonhierarchical categories.

The administrator has the capability to restrict users and login ports to selectable classification ranges. A multi-level mail capability allows users to communicate with each other at classifications defined by the administrator. System V/MLS enforces a security policy that prevents both unauthorized declassification of information and unauthorized modification of trusted code. The mandatory access controls are implemented in a manner analogous to the traditional UNIX commands for discretionary access control. Other commands have been added to allow users to create discretionary groups on the system. Furthermore, users can change levels without having to log out.

A random password generator implements the algorithms recommended in the DoD Password Management Guideline, CSC-STD-002-85. Audit trail records are generated for security-relevant events and can be analyzed by an administrator using an audit trail formatter. A trusted path is provided at login time to ensure that users are communicating with the TCB.

The 630 Multi-Tasking Graphics intelligent terminal (630 MTG), a high-resolution, multi-window graphics terminal, can provide the user with up to seven windows on each of two System V/MLS hosts. The security label of the contents of each window is independent of the labels of other windows. A "cut and paste" capability allows the user to simultaneously edit files at different security levels within the constraints of the enforced security policy.

System V/MLS also provides some features beyond those required for a class B1 system. These include B2 trusted path, B2 subject sensitivity labels, and B2 device labeling. This product participates in the NSA Rating Maintenance Phase (RAMP).

PRODUCT ENHANCEMENTS:

This RAMP action was a bug fix action. Bugs were fixed in the MLS module, and in the following commands: su, newgrp, newpriv, and satfmt.

PRODUCT: System V Release 4.1/ES

VENDOR: UNIX System Laboratory

CANDIDATE CLASS: B2

PRODUCT DESCRIPTION:

UNIX System Laboratories' UNIX System V Release 4.1 Enhanced Security, (hereafter referred to as SVR4.1ES) is a multi-level secure version of UNIX System V for the AT&T 3B2/1000 Model 60 minicomputer. This multi-user, multi-tasking operating system, based on UNIX System V Release 4.0, maintains System V application compatibility, provides BSD and Xenix compatibility, is compatible with the System V Application Binary Interface (ABI) and the SystemV Interface Definition (SVID), passes the System V Verification Suite (SVVS). Applications are source and binary code compatible with existing programs, provided those programs do not require modifications to the SVR4.1ES Trusted Computing Base (TCB) or violate the system security policy. Additionally, SVR4.1ES conforms to the XPG3, IEEE-P1003.1, FIPS151-1, and ANSI C standards.

In addition to using the traditional protection mechanism of the UNIX operating system to provide discretionary access control,SVR4.1ES also provides extended discretionary access controls through the use of access control lists (ACLs) which provide users a mechanism to provide different types of access for each user or group with allowed access. In addition to this discretionary access mechanism, SVR4.1ES provides mandatory access controls to limit the distribution of information to only those users who have been authorized for it. The mandatory security policy is consistent with the Bell-LaPadula model and conforms with DoD policy. SVR4.1ES provides a flexible labeling scheme that supports up to 246 site selectable hierarchical classification levels and 992 nonhierarchical categories.

The administrator has the capability to restrict users and login ports to selectable classification ranges. A multi-level mail capability allows users to communicate with each other at classifications defined by the administrator. SVR4.1ES enforces a security policy that prevents both the unauthorized declassification of information and unauthorized modification of trusted code.

SVR4.1ES provides considerable assurance that the system security features work as specified. Significant effort has been applied to the UNIX System V to create a structured, modular, secure system. Commands have been added to provide security features, and all commands execute with the minimum privilege. SVR4.1ES also provides some features and assurances beyond those required for a class B2 system. These include the use of ACLs to enforce discretionary access controls and a covert channel analysis which provides a thorough search for all covert channels. All of the security features and assurances designed into SVR4.1ES will be evaluated by the Trusted Product and Network Security Evaluation Team.

PRODUCT STATUS:

SVR4.1ES is developed, marketed and supported by UNIX System Laboratories Incorporated. The supporting 3B2/1000 Model 60 hardware is developed and manufactured by the American Telegraph and Telephone Corporation. SVR4.1ES is an enhancement to UNIX System V Release 4.0, which is currently marketed. The evaluated SVR4.1ES is projected to be available in December 1992.

SECURITY EVALUATION STATUS:

A formal evaluation of SVR4.1ES will begin in March 1991 and is scheduled for completion in December 1992. SVR4.1ES will be evaluated against the Department of Defense Trusted Computer System Evaluation Criteria, DAD 5200.28-STD, December 1985.

The Trusted Product and Network Security Division of the National Security Agency considers SVR4.1ES a candidate for the class of products which provide labeled security protection (i.e., class B2). At the completion of the evaluation, a final evaluation report will be produced by the Trusted Product and Network Security Division and SVR4.1ES will be placed on the Evaluated Products List (EPL).

A Product Bulletin does not assign any rating to a product. It establishes the candidate class which is the highest class the system could attain should the formal evaluation be completed. As with all evaluations, a system must complete the formal evaluation phase before being assigned any rating.

ENVIRONMENTAL STRENGTHS:

SVR4.1ES provides isolation of the operating system through its use of the 3B2/1000 hardware protection mechanisms. The hardware supports the two states of the operating system, which are kernel and user level. Kernel level is a privileged level of operation whereby the operating system can protect itself from user intervention. A specific user interface is provided into the kernel, so that operating system services are available to user-level application programs. All memory access is at the kernel level and mandatory as well as discretionary access controls are in force.

Process isolation is guaranteed by the use of per-process virtual address space, memory structures unique to a process and the concept of an active process which has access to controlled kernel resources.

SVR4.1ES provides an auditing facility to ensure user accountability. All security-relevant events are auditable. This facility includes collection, reduction, backup, and data recovery capabilities.

Identification and authentication is accomplished by the trusted login facilities. This mechanism provides for user identification and authentication, and the specification of classification level and categories which determine access to the system itself as well as to application resources. Information about the users (user profiles) is stored in a protected database in SVR4.1ES.

The system also enforces the principle of least privilege for each of the defined privileged user roles (i.e., users should have no more authorization than what is required to perform their functions). The privileged users are assigned to one of the following roles: System Administrator and Trusted System Programmer. Additionally, separate roles can be supported for individuals who require a limited trusted role. This separation is achieved by strictly limiting role activity to predefined operations. In addition, all security-relevant actions performed by privileged users will be audited.

Serial No.CSC-EPL-93/001

EVALUATED PRODUCT: Tandem Guardian 90 with Safeguard

VENDOR: Tandem Computers Incorporated

VERSION: S01.00

DATE: 14 June 1993

OVERALL EVALUATION CLASS: C2

PRODUCT DESCRIPTION:

Tandem NonStop systems are loosely-coupled parallel processor computer systems designed to provide continuous availability for online transaction processing.The combination of NonStop hardware architecture and the Guardian 90 operating system software provides fault-tolerance and data integrity through the following features: multiple independent processors interconnected by dual high-speed internal buses, dual-ported disk drives and device controllers connected to different processors, multiple power supplies, fault tolerant software process pairs in different processors, the transaction monitoring facility software, and failed and run-away hardware and software error detection. All systems provide internal battery backed memory and automatic power-on resumption of processing.

The NonStop hardware architecture defines two processing states which separate privileged Guardian 90 programs from non-privileged user programs. The hardware also enforces virtual-to-real memory mapping, separation of program instruction pages from data pages, and separation of individual user process address spaces.

The Guardian 90 operating system combined with the Safeguard access control product provide security protection mechanisms to mediate access to system resources and prevent object reuse. Discretionary access controls (DAC) can be applied to the following object types: disk volumes, sub volumes, files,devices, subdevices, and processes. The access control lists (ACLSs) can explicitly deny or allow access by specific individuals, by groups of individuals, or both. All individuals, system operators, and security administrators are subject to DAC mechanisms. It is worth noting that in the evaluated configuration, only system administrators are allowed to place ACLs on processes.

Individual user authentication records are maintained by the Safeguard product in a protected file. Designated security administrators create, maintain, and delete user authentication records. Each user has a unique logon ID and password. Each logon ID can have a predefined expiration date or may be temporarily suspended from system usage. Safeguard software provides optional password management features for enforcing minimum length, periodic expiration, minimum change interval, 60 entry history, one-way encryption,invalid password attempts threshold, password expiration warning, and expired password grace period. Upon successful authentication it provides prior logon date and time notification.

The Guardian 90 operating system with the Safeguard product provides an auditing facility that records security-relevant events such as logon and logoff; file open,

close and purge; new process creation; and the use of operator commands. An audit reduction tool is provided to display activity by specific subjects, objects, and time ranges.

The Safeguard product supports three administrative roles to control the use of restricted security commands and definition of controls. The first two roles, defined by the security-administrator and security-operator groups,designate which individuals can use audit service commands, terminal commands,and alter options, as well as stop Safeguard product enforcement. The third role, defined by ownership rules and object-type authorization records,controls the creation and maintenance of subjects, objects, and access privileges. The Safeguard product can be configured to provide a complete audit trail of all administrative changes.

EVALUATION SUMMARY:

The security protection provided by Guardian 90 with Safeguard, configured according the most secure manner described in the Trusted Facility Manual, has been evaluated by the National Security Agency (NSA) against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) dated December 1985.

The NSA evaluation team has determined that the highest class at which Guardian 90 with Safeguard satisfies all specified requirements of the Criteria is class C2. However, it is worth noting that Guardian 90 with Safeguard meets the B3 requirement for DAC and the B1 requirement for system architecture. For a complete description of how Guardian 90 with Safeguard satisfies each requirement of the TCSEC, see Final Evaluation Report, Tandem's Guardian 90 with Safeguard (Report CSC-93/001).

In addition, the report should also be consulted for the complete lists of evaluated hardware and software components.

Serial No.CSC-EPL-92/008

EVALUATED PRODUCT: Tigersafe

VENDOR: ALC A Stealth Group

VERSION: 2K Version: TS3.03.1EN (TS3100)
8K Version: TS8KC (TS8100)

EVALUATION DATE: 30 October 1992

OVERALL EVALUATION CLASS: I&A / D2
OR / D2
DAC / D2
AUD / D2

PRODUCT DESCRIPTION:

Tigersafe is a hardware/software combination that provides Identification & Authentication, Object Reuse, Discretionary Access Control, and Audit functionality. Tigersafe was evaluated on the IBM AT/XT or any 100% IBM compatible clone. It was also evaluated on a Zenith 248 machine and includes features to control access to the Zenith ROM Monitor and Setup utilities. The user plugs the circuit board into any 16 bit slot and installs the software utilities with the provided installation program. The board asserts control as the system is booted by modifying the interrupt vector table. Tigersafe invokes its own code that controls the terminal and keyboard. The net result is a secure login screen that queries the user for a unique password.

The software utilities provide functional control of the Tigersafe environment along with object reuse, discretionary access control and audit capabilities. Tigersafe provides Master Security Administrator and Department Level Administrator utilities that customize the Tigersafe system parameters, initialize users, and set passwords. The utilities also manage user access to the hardware resources (hard disk, disk drive, parallel port, serial port ,communications port, etc.), audit configuration utility, and system setup (ROM Monitor). Usage of the Master Administrator utilities requires an additional authentication step. There are other utilities for users that allow them to change their password and invoke the password banner during normal operation, all with DAC checking and audit provided.

EVALUATION SUMMARY:

The security protection provided by the Tigersafe subsystem has been evaluated against the requirements specified by the Computer Security Subsystem Interpretation (CSSI) of the DoD Trusted Computer System Evaluation Criteria dated September 1988. An I&A subsystem require users to identify themselves to it before they do anything on the system. A subsystem rated as an I&A / D2 system must provide a unique identifier and authenticator for each user. Additionally, it must use those items to control access to the protected system, and must provide an auditing mechanism to log security relevant I&A events.

Tigersafe provides individual user I&A and an event log, which is the combination required to satisfy the functional requirement for Identification and Authentication at the D2 Level of Trust. Tigersafe satisfies the functional requirement for Object Reuse at the D2 Level of Trust by overwriting all data storage objects with ones and zeros prior to initial release to a user.

Tigersafe provides Discretionary Access Control between named users and named objects and controls access to all files, programs and discs associated with the system. The Tigersafe DAC mechanism also allows the user to control access to objects down to the individual and group levels and enforces control over the propagation of these access rights.

Tigersafe provides an Audit mechanism that creates audit trails of all accesses to the protected objects on the system and protects these audit trails with DAC to prevent unauthorized access (read / write) or destruction.All I&A events, object deletions, user actions, System Administrator actions and all other security related events are audited. The time, date, event type, and success or failure of each action are logged in one of five audit trails provided within the Tigersafe subsystem.

In addition to meeting the functionality requirements and interpretations defined in the CSSI, subsystems must also meet the assurance and documentation requirements. Tigersafe satisfies all assurance and documentation requirements as outlined in the CSSI. The evaluation team has determined that the Tigersafe subsystem meets all the specific requirements of the CSSI to achieve an overall D2 Level of Trust. For complete description of how the Tigersafe system satisfies each requirement of the CSSI, see Final Evaluation Report, ALC Tigersafe (Report No. CSC-EPL-92/008).

Serial No. CSC-EPL-85/002

EVALUATED PRODUCT: TOP SECRET

VENDOR: CGA Software Products Group, Inc.

VERSIONS: Version 3.0 Level 163 with Feature Option \#43

DATE: 2 April 1985

OVERALL EVALUATION CLASS: C2

PRODUCT DESCRIPTION:

TOP SECRET is an add-on security package developed by CGA Software Products Group, Inc. for IBM's Multiple Virtual Storage (MVS) operating system. TOP SECRET provides default protection of system facilities, data sets resident on DASD devices, and DASD and tape volumes. TOP SECRET also provides the capability for decentralized access control through several layers of security administration, extensive audit features (both on-line and batch), and the capability to gradually implement the security provided by the TOP SECRET package.

Interfaces between TOP SECRET and many commercial software products are provided by CGA. These include: Information Management System (IMS), Customer Information Control System (CICS), ROSCOE, COMPLETE, TSO, IDMS, PANVALET, and others.

EVALUATION SUMMARY:

TOP SECRET Version 3.0 Level 163 running with IBM's Multiple Virtual Storage/System Product (MVS/SP) operating system has been evaluated by the Department of Defense Computer Security Center (DoDCSC). The security provided by TOP SECRET was evaluated against the requirements specified in the Department of Defense Trusted Computer System Evaluation Criteria (the Criteria) dated 15 August 1983.

The DoDCSC's evaluation team has determined that the highest class for which TOP SECRET Version 3.0 satisfies all the requirements of the Criteria is class C2. Note that this rating is applicable only to TOP SECRET configured as detailed in the final evaluation report. TOP SECRET does not satisfy the requirements for any of the B levels as it does not provide labelling capabilities and thus does not possess a mandatory access control mechanism.

A class B1 rating is considered attainable but would require a significant amount of work to implement the necessary mechanisms. TOP SECRET could not, however, evolve to a class higher than B1 without a major reimplementation of the majority of the MVS operating system and its subsystems.

At the time of the evaluation, TOP SECRET Version 3.0 ran only with the MVS operating system. The overall integrity of the TOP SECRET package is directly dependent upon the integrity of the MVS system itself.

The figure above indicates the requirements and corresponding level that TOP SECRET/MVS satisfies. The rating given to the evaluated system (viz., C2) is the highest level of the Criteria at which the system satisfies all the specified requirements. The "range of feasible use" is intended to convey the overall system integrity level of the system as it is delivered by the vendor and indicates that this system could be used in an environment requiring an evaluation class within this range so long as the missing features, if any, are not essential to the operational capability. For a complete description of how TOP SECRET/MVS satisfies each requirement of the Criteria, see Final Evaluation Report, TOP SECRET Version 3.0 (Report No. CSC-EPL-85/002).

Serial No. CSC-PB-94/002

AS OF: 26 July 1994

PRODUCT: Trusted IRIX/B

VENDOR: Silicon Graphics Computer Systems, Inc.

VERSION: Release 4.0.5EPL

CANDIDATE CLASS: B1 (TCSEC)

PRODUCT DESCRIPTION:

Trusted IRIX/B Release 4.0.5EPL is a distributed system of Silicon Graphics Computer Systems, Inc. (SGI) IRIS Indigo/Entry Graphics workstations interconnected via an Ethernet. These UNIX-based multi-user, multi-tasking workstations provide general purpose computing, 3-D graphics, 2-D graphics, video, and audio support. The processor of the evaluated Trusted IRIX/B system workstation is the MIPS R4OOOSC. This distributed system supports TCP/IP network protocols and services for communication between workstations.

Trusted IRIX/B is a security-enhanced version of IRIX 4.0, the IRIS Indigo multi-user, multi-tasking operating system. In addition to using the traditional discretionary access control (DAC) mechanisms provided by UNIX-based systems, Trusted IRIX/B provides mandatory access control (MAC) to restrict the flow of information based on the sensitivity and the integrity of the information and the clearance of the user attempting to access the information. Trusted IRIX/B implements a label-based MAC policy based on the Bell and LaPadula model for sensitivity and the Biba model for integrity. A flexible labeling scheme allows up to 256 sensitivity levels and 65536 categories and a like number of integrity grades and divisions. (Grades and divisions are analogous to sensitivity levels and categories.) An individual label may contain a combined total of 250 categories and divisions. The security policy also prevents both the unauthorized declassification of user informagwon and unauthorized modification of trusted code. The integrity component of the MAC label is used as an identification and isolation mechanism for the TCB. It is also used to identify users with administrative roles.

Trusted IRIX/B includes a DAC policy on sockets. This policy allows a sending process to send data to a socket only if the user that created the sending socket is included in an access control list associated with the target socket.

Trusted IRIX/B offers an X Window interface that supports one user operating at a single label at a time. It enforces this restriction with its MAC and DAC mechanisms.

Trusted IRIX/B provides for user identification and authentication through user identifiers and passwords. All workstations in the system share the same identification and authentication database using the Network File System (NFS) facility. The administrator can allow users to choose their own passwords or may choose to require the use of a

Trusted IRIX/B-provided password generator. The administrator also can restrict users to selectable classification ranges.

Users may communicate with each other using one or more single-level mailboxes at classifications configured by the administrator. Audit trails of security relevant activities are generated for actions taken on all workstations on the system to provide user-level accountability. System-level and workstation-specific audit trails can be analyzed by the administrator using provided audit reduction tools.

The National Computer Security Center (NCSC) considers the Trusted IRIX/B system a candidate for a B1 rating under the Dad Trusted Computer System Evaluation Criteria. A system that is rated as being a B1 class system provides a TCB that preserves the integrity of sensitivity labels, and uses them to enforce a set of MAC rules. B1 systems also provide DAC, identification and authentication, object cleansing between uses, and auditing facilities. Assurance is provided primarily through design analysis and testing.

Trusted IRIX/B is being maintained under configuration management in accordance with the NCSC Ratings Maintenance Program, and it is anticipated that it will continue to be maintained in accordance with this program.

PRODUCT STATUS:

Trusted IRIX/B is being developed and is supported as a commercial off-the-shelf product by Silicon Graphics Computer Systems Inc., Mountain View, California.

SECURITY EVALUATION STATUS:

A formal evaluation of Trusted IRIX/B began in July of 1994 and is scheduled for completion in fourth quarter of 1994. At the completion of the formal evaluation, the NCSC will produce a final evaluation report, and place Trusted IRIX/B on the Evaluated Product List. Trusted IRIX/B will be evaluated against the B1 class requirements of the TCSEC.

A Product Bulletin does not assign any rating to a product. It merely establishes the candidate class which is the highest class the system could obtain should formal evaluation be completed. As with all evaluations, a system must complete the formal evaluation phase before being assigned any rating.

Serial: CSC-EPL-94/004

EVALUATED PRODUCT: Trusted Oracle 7

VENDOR: Oracle Corporation

RELEASE: 7.0.13.1 with the Procedural Option

DATE: 5 April 1994

OVERALL EVALUATION CLASS: B1

PRODUCT DESCRIPTION:

Trusted Oracle7 provides all of the advanced cooperative server technology present in Oracle's base product Oracle7 (itself evaluated at Class C2), with the addition of multilevel security and labeled data management. All of the Oracle7 features are included in Trusted Oracle7 and enhanced where necessary for multilevel security. Trusted Oracle7 is certified by NIST as 100% compliant for ISO5057/ANSI SQL89 level 2 including the integrity enhancement feature. Trusted Oracle7 includes support for stored procedures, triggers, declarative integrity constraints, synonyms, asynchronous replication, and resource limits.

Trusted Oracle7 applies the mandatory access control (MAC) security policy of the underlying operating system to database activity and objects. Trusted Oracle7 uses sensitivity labels as the basis for mandatory access control. Trusted Oracle7 can be configured in either of two modes: DBMS MAC or OS MAC mode. DBMS MAC mode relies on the MAC label definitions and MAC policy provided by the underlying operating system. Trusted Oracle7 applies these labels to database rows and enforces the policy within the database. In OS MAC mode, only the underlying operating system enforces MAC security policies on single-level storage objects at the file level. Each database is single level; however, users can read information from lower level databases.

Trusted Oracle7 provides authentication via the identification and authentication mechanism of the underlying operating system.The label at which the user is operating and the clearance range of the user is obtained from the operating system.

Discretionary access control in Trusted Oracle7 is achieved through the use of privileges. The privileges come in two forms: object and system privileges. Object privileges control access to particular database objects. System privileges control use of SQL commands. In order to facilitate privilege administration, Trusted Oracle7 privileges can be grouped in roles. Roles are defined groups of privileges that can be granted to users and other roles. Trusted Oracle7 in DBMS MAC mode provides additional privileges that apply to MAC: readup, writeup, and writedown. These privileges can be granted to a user or a role.

Trusted Oracle7 provides a highly configurable set of auditing capabilities. Trusted Oracle7 provides the ability to selectively audit very specific operations by narrowing the scope of the audit to only the desired information, thereby reducing the

system resources needed for auditing. Application specific auditing can be implemented using Trusted Oracle7 triggers. In addition, all audit records include the MAC label of the process causing the audit record to be generated as well as the MAC label of the relevant object.

Trusted Oracle7 provides extensive data integrity features in addition to its security features. Trusted Oracle7 uses row-level locking and multi- version read consistency to provide high performance concurrency controls. Declarative integrity constraints and trigger procedures can be used to assure that the data maintained by Trusted Oracle7 is constrained by the business rules defined for the database.

EVALUATION SUMMARY:

Trusted Oracle7 was evaluated against the "DoD Trusted Computer System Evaluation Criteria", DoD 5200.28-STD, dated December, 1985 as interpreted by the "Trusted Database Interpretation of the Trusted Computer System Evaluation Criteria", dated April 1991 as a B1 class database management system.

The NSA evaluation team has determined that the highest class at which Trusted Oracle7 running on HP-UX BLS satisfies all specified requirements of the Criteria is class B1. For a complete description of how Trusted Oracle7 running on HP-UX BLS satisfies each requirement of the TCSEC and TDI, see the Final Evaluation Report, Oracle Corporation Oracle7 and Trusted Oracle7 (Report CSC-EPL-94/003).

Oracle Corporation has satisfied the requirements for participation in the Ratings Maintenance Program (RAMP) and it is anticipated that ports to additional platforms will be evaluated under RAMP.

Serial No.CSC-EPL-92/006

EVALUATED PRODUCT: Trusted OS/32 with OS/32 MTM

VENDOR: Concurrent Computer Corporation

VERSION EVALUATED: Release 08.03-3S

EVALUATION DATE: 1 October 1992

OVERALL EVALUATION CLASS: C2

PRODUCT DESCRIPTION:

OS/32 is Concurrent's real-time operating system that runs on all of its single and multiprocessing Series 3200 systems and 8/32 systems. OS/32 Mufti-Terminal Monitor (OS/32 MTM) is Concurrent's timesharing and program development environment that runs on OS/32. Together they provide a trusted development and real-time environment from small scale dedicated systems to large scale multiprocessing systems. These products have been evaluated on Concurrent's 3280, 3280E, and all members of Concurrent's Micro 3200 family.

Trusted OS/32 with OS/32 MTM provides discretionary access control on user accounts, thereby providing read and write access control to the granularity of the collection of the account's files. In addition, Concurrent's restricted disks capability limits access to selected disks only to users with appropriate access privileges. The system administrator can also "cloak"certain devices from selected users, thereby preventing the user from accessing or even knowing that a given device is available.

Trusted OS/32 with OS/32 MTM also provides user identification and authentication through user account numbers and passwords. Tailorable site-specific security measures or system administration procedures can be executed during logon and logoff by command files established by the system/security administrator. Individual accountability is obtained through the system's ability to audit each user's security relevant events.

Compliance with the object reuse requirement is accomplished by overwriting physical memory before it is allocated to another user. Disk blocks are overwritten upon allocation of a file and optionally overwritten when a file is deallocated.

EVALUATION SUMMARY:

The security protection provided by Trusted OS/32 with OS/32 MTM, configured according to the most secure manner described in the Trusted Facility Manual,has been evaluated by the National Security Agency (NSA) against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria, dated December 1985.

The evaluation team has determined that the highest class at which OS/32 satisfies all the specified requirements of the Criteria is class C2. In addition, OS/32 satisfies the functionality of the B1 requirement for System Architecture.

For a complete description of how Trusted OS/32 with OS/32 MTM satisfies each requirement of the Criteria, see Final Evaluation Report, Concurrent Computer Corporation, OS/32 Release 8.3.3S (Report No. CSC-EPL-92/006).

PRODUCT: Trusted Solaris

VENDOR: Sun Microsystems Federal, Inc.

CANDIDATE CLASS: B1

PRODUCT DESCRIPTION:

Trusted Solaris Version 1.1 is a multilevel trusted version of the SunOS Version 4.1.3(1) that incorporates trusted versions of Open Windows Version 3.0--which is a combination of the X Window System 11R4 and NeWS window system--and the Open Look Window Manager. Trusted Solaris is a general-purpose, multi-tasking operating system with a windowing system in a distributed environment. The security and functional enhancements required by the Trusted Computer System Evaluation Criteria (TCSEC) and the Compartmented Mode Workstation Requirements have been added to SunOS Version 4.1.3.

Sun Microsystems Federal develops and markets Trusted Solaris Version 1.1 for the following SPARC(2) machines:

- System 4/25 SPARCstation ELC
- System 4/50 SPARCstation IPX
- System 4/60 SPARCstation 1
- System 4/65 SPARCstation 1+
- System 4/75 SPARCstation 2
- SPARCstation 10 model 51 (uniprocessor)
- System 4/470 SPARCserver 470
- System 4/490 SPARCserver 490
- SPARC server 690MP with SuperSPARC (uniprocessor)

SECURITY EVALUATION STATUS:

A formal evaluation of Trusted Solaris will commence in October of 1994 and is scheduled for completion in the third quarter of 1995. Trusted Solaris will be evaluated against the TCSEC as a B1 system (Labeled Security Protection). At the completion of the evaluation, a final evaluation report will be published by the National Computer Security Center, and Trusted Solaris will be placed on the Evaluated Products List.

In conjunction with the TCSEC evaluation, the system is also being evaluated against the Compartmented Mode Workstation (CMW) requirements of the Security Requirements for System High and Compartmented Mode Workstations (CMWREQs). At the completion of the CMW evaluation, Trusted Solaris will also be placed on the TCB Extensions List as a CMW. The TCB Extensions List will be available in future publications of the Information Systems Security Products and Services Catalogue.

A Product Bulletin does not assign any rating to a product. It merely establishes the candidate class, which is the highest class the system could attain when the

formal evaluation is complete. As with all evaluations, a system must complete the formal evaluation phase before being assigned any rating.

ENVIRONMENTAL STRENGTHS:

Trusted Solaris provides security for environments requiring a homogeneous distributed system. All elements of this distributed system (i.e., workstations and servers) have equal system accreditation ranges. Trusted Solaris provides trusted Open Windows which labels each window in a trusted banner. Open Windows contains a trusted path mechanism for login and for performing all security-relevant functions.

Trusted Solaris provides user identification and authentication through user names and passwords, and individual accountability through its auditing mechanisms. The authentication features of the CMW comply with the guidelines recommended in the Dad Password Management Guideline, CSC-STD-002-85. The auditing mechanism support preselection and post-selection by user, group, event and sensitivity level range.

Trusted Solaris provides the traditional user specified access controls (i.e., discretionary access controls) through protection bits and access control lists. In addition, Trusted Solaris provides mandatory access controls to control the distribution of information protected by the system to only those users who have been authorized for the information. Trusted Solaris enforces an information labeling policy on the information contained in objects. Information labels are not used for access control checks.

The system supports three separate privileged user roles as defined in the CMWREQs for maintaining the system: System Administrator, Information System Security Officer (ISSO) and Operator. Trusted Solaris supplies a privilege mechanism and a large number of discrete privileges that may be used to implement the principle of least privilege at the user level. A set of desk set tools with the ability to run multiple windows and tools at different labels at the same time is also provided by Trusted Solaris, as is multi-level cut and paste. Trusted Solaris also provides users the ability to print PostScript files in a trustworthy manner.

(1) Sun, Sun Microsystems, SunOS, Solaris, Trusted Solaris, NeWS, NeWSprint,and Open Windows are trademarks or registered trademarks of Sun Microsystems,Inc. UNIX and OPEN LOOK are registered trademarks of UNIX System Laboratories, Inc., a wholly owned subsidiary of Novell, Inc. The X Windows System is a trademark of the Massachusetts Institute of Technology. All other product names mentioned herein are the trademarks of their respective owners.
(2) All SPARC trademarks, including the SRD Compliant Logo, are trademarks or registered trademarks of SPARC International, Inc.SPARCstation, SPARCserver, and SPARC printer are licensed exclusively to Sun Microsystems, Inc. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

Serial No: CSC/EPL/94/002

EVALUATED PRODUCT: Trusted UNICOS 8.0

VENDOR: Cray Research, Inc.

VERSION EVALUATED: Release 8.0.2

EVALUATION DATE: 09 March 94

OVERALL EVALUATION CLASS: B1 MDIA (TNI)

PRODUCT DESCRIPTION:

The Trusted UNICOS 8.0 operating system from Cray Research, Inc. is a multilevel secure (MLS) version of Cray Research's UNICOS operating system. The UNICOS operating system is a general purpose, time-sharing, computer operating system based upon the UNIX System V operating system of UNIX System Laboratories, Inc. It incorporates extensive network connectivity based on the Fourth Berkeley Software Distribution under license from the Regents of the University of California. The Trusted UNICOS 8.0 system is a specifically defined configuration of the UNICOS operating system with MLS and security options configured according to the instructions in the Trusted Facility Manual. Trusted UNICOS runs on CRAY Y-MP supercomputer systems, including the C90 series, M90 series, E series, and EL series supercomputers. Because CRAY Y-MP computer systems do not support directly connected users, the Trusted UNICOS 80 system is evaluated as an MDIA Network Component. The Trusted UNICOS 8.0 system is designed to operate in a heterogeneous networked environment and can maintain its evaluated rating when integrated into a heterogeneous network trusted computing base (NTCB).

The Trusted UNICOS 8.0 system provides discretionary access control(DAC) mechanisms based on file permission bits and access control lists(ACLs). ACLs provide a finer granularity of DAC control than file permission bits provide. The Trusted UNICOS 8.0 system also provides mandatory access controls (MAC) based on sensitivity labels for subjects and objects. MAC features include: file system object labeling; multilevel directories; multilevel mail; and the use of the Internet Protocol (IP) Basic Security Option (BSO) and the Common IP Security Option (CIPSO) to support packet labeling across the network.

Identification and authentication use passwords and a number of configurable features, which allow a site to control and monitor user access to the Trusted UNICOS 8.0 system. Optionally, the Security Dynamics SecurID one-time password card is supported to provide an additional form of access authorization. The auditing capabilities of the Trusted UNICOS 8.0 system provide configurable options for recording security-relevant events, such as object creation and access attempts, in an audit trail. A utility to view the audit trail data is provided.

The Trusted UNICOS 8.0 system provides trusted facility management through a mechanism that allows users to be granted access to a defined operator role that has limited capabilities and is distinct from other administrative roles. The Trusted UNICOS

8.0 system is also designed to minimize privileges employed within the trusted computing base (TCB) through a fine-grained privilege mechanism.

TCP/IP, UDP, RPC, NFS, and the Network Queuing System (NQS) product are the major networking components supported in the Trusted UNICOS 8.0 system. The BSO and CIPSO protocols are supported at the IP layer providing packet labeling across a network. Also supported is the mapping of labels, which allows connections to other trusted systems in a heterogeneous NTCB. The following network services and protocols rely and build on BSO and CIPSO to maintain object labels across a network: TCP/IP, UDP, RPC, NFS, NQS, telnet, rlogin, rexec, rsh, rcp, ftp, lpd, sendmail, and user sockets.

The tape subsystem provides for the secure handling of labeled tapes.The Cray/REEL librarian product keeps track of tape volume and file security attributes. The Cray Data Migration Facility subsystem provides for the off-line storage of Trusted UNICOS files. It provides automatic backup and restore of files to protected tape volumes.

For connection to Ethernet, FDDI, and HYPER channel networks on the CRAYY-MP supercomputer systems, the Trusted UNICOS 8.0 configuration includes the 7300-XX, 7402-XX, and 7404-XX Series Data Exchange (DX and DXE) Cray Research System host controllers from Network Systems Corporation. Nine models of the 7300, 7402, and 7404 Cray Host Controllers are included: the 7300-21, 7300-32, and 7300-62 are used with the CRAY C90, M90, and E series supercomputers while the 7402-21,7402-32, 7402-62, 7404-21, 7404-32, and 7404-62 are used with the CRAY EL series supercomputers.

For the CRAY EL series supercomputers, the 7402 or 7404 controllers are not required for connections to Ethernet or FDDI networks. The Ethernet controller is a standard piece of hardware on the CRAY EL series supercomputers. An FDDI IOS controller is necessary for FDDI network connections.

The Trusted UNICOS 8.0 system also supports network connections between Cray Research systems via the High Performance Parallel Interface (HIPPI).

The Trusted UNICOS 8.0 configuration optionally includes the ACM/7100 system from Security Dynamics, Inc. as an authentication mechanism. This system supports the SD100, SD200, SD510, and SD520 SecurID cards.

Other major Cray Research products included in the Trusted UNICOS 8.0 TCB are the I/O Subsystem Model E (IOS-E), Secondary Storage Device (SAD-E), the operator workstation (OWS-E), the maintenance workstation(MWS-E), tape subsystem support, Cray Data Migration Facility (DMF) subsystem support, and the Cray/REEL librarian (CRL) product.

The OWS and MWS are Sun-4/370 Workstations (SPARC station) running the SunOS operating system. The OWS supports a captive interface that provides administrative access to CRAY C90 series, M90 series, and E series supercomputers. The MWS provides an on-line maintenance platform that includes on-line diagnostics, maintenance commands and utilities, and a hardware error logging capability.

EVALUATION SUMMARY:

The securigw protection provided by the Trusted UNICOS 8.0 system, when configured in a B1-compliant manner as described in the Trusted Facility Manual, was evaluated by the National Security Agency (NSA) against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria (DOD 5200.28-STD) dated December 1985 as interpreted in the Trusted Network Interpretation dated July 1987.

The NSA evaluation team has determined that the highest class at which the Trusted UNICOS 8.0 system satisfies all the specified requirements of the Criteria is class B1 MDIA network component. For a complete description of how the Trusted UNICOS 8.0 system satisfies each requirement of the Criteria, see Final Evaluation Report, Cray Research, Inc. Trusted UNICOS 8.0 Operating System (Report CSC-94/002).

In addition to the Trusted UNICOS 8.0 features that meet the B1 MDIA requirements, functional aspects of several higher level requirements are met: B3 discretionary access control (DAC), B2 trusted facility management, and A1 trusted distribution. However, no assurance above the B1 class is provided.

SERIAL NO.CSC-EPL-SUM 91/003

EVALUATED PRODUCT: Trusted XENIX

VENDOR: Trusted Information Systems, Inc.(TIS)

VERSION EVALUATED: Trusted XENIX Version 2.0

EVALUATION DATE: 9 January 1991

OVERALL EVALUATION CLASS: B2

PRODUCT DESCRIPTION:

Trusted XENIX Version 2.0 (Trusted XENIX) is a trademark of the Microsoft Corporation. It is a UNIX-like, multi-level secure operating system for the IBM Personal Computer AT (PC AT),and IBM Personal System/2 (PS/2) Models 50, 60, 70, 70T, 70P and 80. IBM Personal Computer AT and Personal System/2 are registered trademarks of the IBM Corporation. It is a multi-user, multi-tasking system which can support up to six concurrent users using currently available IBM equipment. Trusted XENIX contains many functional and security enhancements while maintaining binary compatibility with programs developed under IBM Personal Computer XENIX versions 1.0 and 2.0.

Trusted XENIX is designed to provide a high level of security for environments requiring trusted desktop data processing. Trusted XENIX enforces a mandatory security policy based on the Bell and LaPadula security model. Discretionary access controls include traditional UNIX (UNIX is a registered trademark of AT&T Bell Laboratories, Inc.) protection bits, as well as Access Control Lists. Trusted XENIX performs user identification and authentication, generates audit trail records, and provides abase upon which to build secure application programs. Evaluated hardware configurations include a range of disks, disk controllers, video configurations, and a cartridge tape unit for fast system back-up and restore.

The system enforces the "principle of least privilege" (i.e.,users should have no more authorization than what is required to perform their functions) for each of the four defined privileged user roles available in multi-user mode. These privileged users are assigned to one of the four following roles: System Security Administrator, Secure Operator, Account Administrator, and Auditor. This separation is supported by strictly limiting privileged users to predefined operations. In addition, allocations performed by privileged users can be audited, and the audit log cannot be modified by unprivileged users, the System Security Administrator, Secure Operator, or Account Administrator. In addition, there is also a Trusted System Programmer who is responsible for initial hardware and system configuration. This role only exists in single-user mode.

EVALUATION SUMMARY:

The security protection provided by Trusted XENIX, configured according to the most secure manner described in the Trusted Facility Manual, has been evaluated by the National Computer Security Center (NCSC) against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria [DOD 5200.28-STD] dated December 1985.

The NCSC evaluation team has determined that the highest class at which Trusted XENIX satisfies all the specified requirements ofthe Criteria is class B2. In addition, Trusted XENIX satisfies the functionality of the B3 requirements for DAC, Trusted Path, and Trusted Facility Management.

For a complete description of how Trusted XENIX satisfies each requirement of the Criteria, see Final Evaluation Report, Trusted Information Systems' Trusted XENIX (Report CSC-91/003).

In addition, the report should also be consulted for the complete lists of evaluated hardware and software components.

Serial No. CSC-EPL-92/001

EVALUATED PRODUCT: Trusted XENIX

VENDOR: Trusted Information Systems, Inc. (TIS)

VERSION EVALUATED: Trusted XENIX Version 3.0

EVALUATION DATE: 8 April 1992

HARDWARE PLATFORMS:

AST 386/25; GRID 1537; IBM PC AT; IBM PS/2 - Models 50, 60, 70, 70T, 70P, and 80; NEC PowerMate 386/25; NEC BusinessMate 386/25; Unisys Personal Workstation 2 Series 800; Zenith Z-386/33.

OVERALL EVALUATION CLASS: B2

PRODUCT DESCRIPTION:

Trusted XENIX version 3.0 is a UNIX-like, multi-level secure operating system that has been enhanced (from Trusted XENIX version 2.0) to include the platforms listed above. It is a multi-user, multi-tasking system. Trusted XENIX contains many functional and security enhancements while maintaining binary compatibility with programs developed under IBM Personal Computer XENIX versions 1.0 and 2.0. (XENIX is a trademark of Microsoft Corporation).

Trusted XENIX is designed to provide a high level of security for environments requiring trusted desktop data processing. Trusted XENIX enforces a mandatory security policy based on the Bell and LaPadula security model. Discretionary access controls include traditional UNIX protection bits, as well as Access Control Lists. Trusted XENIX performs user identification and authentication, generates audit trail records, and provides a base upon which to build secure application programs. Evaluated hardware configurations include a range of disks, disk controllers, video configurations, and a cartridge tape unit for fast system back-up and restore. (UNIX is a registered trademark of AT&T Bell Laboratories, Inc.).

The system enforces the "principle of least privilege" (i.e., users should have no more authorization than what is required to perform their functions) for each of the four defined privileged user roles available in multi-user mode. These privileged users are assigned to one of the four following roles: System Security Administrator, Secure Operator, Account Administrator, and Auditor. This separation is supported by strictly limiting privileged users to predefined operations. In addition, all actions performed by privileged users can be audited, and the audit log cannot be modified by unprivileged users, the System Security Administrator, Secure Operator, or Account Administrator. In addition, there is also a Trusted System Programmer who is responsible for initial hardware and system configuration. This role only exists in single-user mode.

EVALUATION SUMMARY:

The security protection provided by Trusted XENIX, configured according to the most secure manner described in the Trusted Facility Manual, has been evaluated by the National Security Agency (NSA)against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria [DOD 5200.28-STD] dated December 1985.

The evaluation team has determined that the highest class at which Trusted XENIX satisfies all the specified requirements of the Criteriais class B2. In addition, Trusted XENIX satisfies the functionality of the B3 requirements for DAC, Trusted Path, and Trusted Facility Management.

For a complete description of how Trusted XENIX satisfies each requirement of the Criteria, see Final Eva

RATING MAINTENANCE PRODUCT: Trusted XENIX Version 4.0

ORIGINAL EVALUATED PRODUCT: Trusted XENIX

VENDOR: Trusted Information Systems, Inc. .

RATING MAINTENANCE DATE: 17 September 1993

EVALUATED PLATFORMS: AST 386/25 and Premium 386/33; GRiDCASE 1537 and GRiD 386sx-M Workstation 2 Series 800/20C; Wang 382 and 382T; and Zenith Z-386/33

OVERALL EVALUATION CLASS: B2

PRODUCT DESCRIPTION:

Trusted XENIX version 4.0 is a UNIX-like, multi-level secure operating system that has been enhanced (from Trusted XENIX version 3.0) to add a new remote connection capability for use with STU-IIIs, to include seven additional hardware platforms, and to provide bug fixes. It is a multi-user, multi-tasking system. Trusted XENIX contains many functional and security enhancements while maintaining binary compatibility with programs developed under IBM Personal Computer XENIX versions 1.0 and 2.0.

Trusted XENIX is designed to provide a high level of security for environments requiring trusted desktop data processing or MLS interfaces. Trusted XENIX enforces a mandatory security policy based on the Bell and LaPadula security model. Discretionary access controls include traditional UNIX protection bits, as well as Access Control Lists. Trusted XENIX performs user identification and authentication, generates audit trail records, and provides a base upon which to build secure application programs. Evaluated hardware configurations include a range of disks, disk controllers, video configurations, and a cartridge tape unit for fast system back-up and restore.

The system enforces the "principle of least privilege" (i.e., users should have no more authorization than that required to perform their functions) for each of the four defined privileged user roles available in multi-user mode. These privileged users are assigned to one of the four following roles: System Security Administrator, Secure Operator, Account Administrator, and Auditor. This separation is supported by strictly limiting privileged users to predefined operations. In addition, all actions performed by privileged users can be audited, and the audit log cannot be modified by unprivileged users, the System Security Administrator, Secure Operator, or Account Administrator. In addition, there is also a Trusted System Programmer who is responsible for initial hardware and system configuration. This role exists only in single-user mode.

The remote connection capability of Trusted XENIX is implemented in a server/client configuration. The server consists of a serial device driver that monitors the trusted XENIX to STU-III data port connection, and a trusted process that ascertains and then sets the serial port label to the negotiated key level between the STU-IIIs. The client consists of

four trusted processes that establish a connection, invoke the server's trusted shell, disconnect the session, as well as monitor the STU-III and its connections. These Trusted XENIX functions have been evaluated against the class B2 criteria using three AT&T STU-IIIs: the Security Plus, the 1900 Secure Data Device, and the 1100 Secure Voice/Data Terminal. Note, however, that though these functions have been evaluated, none of the STU-III devices has been similarly evaluated. Rather, certain assumptions have been made regarding the STU-III device interfaces and the functions that they provide in order to effectively evaluate Trusted XENIX.

EVALUATION SUMMARY:

The security protection provided by Trusted XENIX, configured according to a secure manner described in the Trusted Facility Manual, has been evaluated by the National Security Agency (NSA) against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria [DOD 5200.28-STD] dated December 1985.

The evaluation team has determined that the highest class at which Trusted XENIX satisfies all the specified requirements of the Criteria is class B2. In addition, Trusted XENIX satisfies the functionality of the B3 requirements for DAC, Trusted Path, and Trusted Facility
Management.

For a complete description of how Trusted XENIX satisfies each requirement of the Criteria, see Final Evaluation Report, Trusted Information Systems, Trusted XENIX Version 4.0 (Report No. CSC-EPL-92/001.A).

REPORT NO:CSC-PB-93/002

AS OF: 21 April 1993

PRODUCT: ULTRIX MLS+

VENDOR: Digital Equipment Corporation

CANDIDATE CLASS: B1/CMW

PRODUCT DESCRIPTION:

Digital Equipment Corporation's ULTRIX MLS+ Trusted Worksystem Software is a general purpose multi-user UNIX operating system based on Digital's ULTRIX...

Basic discretionary access controls are provided by the traditional UNIX user categories (owner, group, other); and access control lists that contain identifiers for users and groups of users with the authorized access for the identifier. A user may be associated with a number of different identifiers ,providing a flexible mechanism for grouping access permissions based on identifiers.

Mandatory access controls support access mediation based on sensitivity labels associated with both data and users. MLS+ objects that can be shared among users, files for example, are protected by mandatory access controls.

Information labels more accurately reflect the actual sensitivity of pieces of information within data containers. They contain the same classifications and compartments as do sensitivity labels; but also contain non-hierarchical markings. These are automatically adjusted by the system as necessary.

These access controls apply not only to the file system and interprocess communicatgwns but to the window system as well. This means that inter-window data transfers are controlled. Also, users may choose the sensitivity level at which to run X windows applications.

Security administration features provided by MLS+ include support for user registration with password management options, audit collection and analysis, and delegation of administrative authority using MLS+ system privileges.

Other features included are: labeling of all objects, a trusted path, trusted facility management, and extended configuration management.

ULTRIX MLS+ is being evaluated on the VAX architecture. Protection mechanisms are supported by hierarchical hardware modes. Memory access and protection; and process isolation are based on those modes. In addition, privileged instructions provide hardware protection.

PRODUCT STATUS:

ULTRIX MLS+ is developed, marketed, and supported by Digital Equipment Corporation. The current version of ULTRIX MLS+ is V1.0a; the evaluated version is scheduled to be V2.0 available in September 1993.

SECURITY EVALUATION STATUS:

A formal evaluation of ULTRIX MLS+ began in April 1993 and is scheduled for completion in November 1993. ULTRIX MLS+ will be evaluated against the Department of Defense Trusted Computer System Evaluation Criteria, December 1985; and the Defense Intelligence Agency Compartmented Mode Workstation Requirements, DDS-2600-5502-87.

The Trusted Product Evaluation Division of the National Security Agency considers ULTRIX MLS+ a candidate for the class of products that provide labeled security protection, where data is labeled and access is controlled based on those labels (i.e., class B1). The Defense Intelligence Agency considers ULTRIX MLS+ a candidate for Compartmented Mode Workstation class of products. At the completion of the formal evaluation, a final evaluation report will be provided by the Trusted Product Evaluation Division and the Defense Intelligence Agency and ULTRIX MLS+ will be placed on the Evaluated Product List (EPL).

A Product Bulletin does not assign any rating to a product. It establishes the candidate class which is the highest class the system could attain should the formal evaluation be completed. As with all evaluations, a system must complete the formal evaluation phase before being assigned any rating.

ENVIRONMENTAL STRENGTHS:

ULTRIX MLS+ provides a flexible discretionary access control mechanism using ACL's that can be used to define complex controls for sharing access. Account restrictions can be specified by an administrator to provide flexible controls on the environment and system resources accessible to individual users. The mandatory controls of ULTRIX MLS+ provide access mediation using data sensitivity labels. These controls apply to the X windowing system as well.

Subject: EPL Networks SERIAL NUMBER: CSC-EPL-SUM-90/001

EVALUATED PRODUCT: VSLAN 5.0

VENDOR: General Kinetics Corporation (Formerly Verdix)

EVALUATION DATE: 25 July 1990

OVERALL EVALUATION CLASS: B2 MDIA Network Component

PRODUCT DESCRIPTION:

The Verdix Secure Local Area Network (VSLAN) is a network component that is capable of interconnecting host systems operating at different ranges of security levels allowing a multi-level secure (MLS) LAN operation. The VSLAN is not intended to be a network system. It can be used to build and support a class B2 network system when included in the proper network system architecture. The VSLAN operates at the physical and data-link protocol layers of the Open Systems Interconnection (OSI) reference model, independently of higher-layer, host-to-host protocols. Because of the VSLAN's independence of these upper layer protocols, it can be used to integrate a variety of host systems ranging from DoD internet gateways to vendor-specific systems.

The VSLAN consists of a single Network Security Center (NSC) and up to 128 Network Security Devices (NSDs) interconnected by a transmission medium (i.e., coaxial cable). The NSC is a dedicated computer system that provides a centralized management facility. The NSC supports separate administrator and operator roles. It provides a menu-driven interface for the security officer (i.e., administrator and/or operator) to control the operation of the VSLAN and to collect and store audit data.

Each NSD operates as an individual node of the VSLAN, providing a trusted network interface for its attached host that provides the LAN communications (IEEE 802.3) and enforces the VSLAN security policy for all host-to-host data transfers. Each NSD provides a system bus interface to its attached host and acts as a memory device on its host bus. In order to integrate the NSD with the host operating system, host-specific software is needed to make use of the trusted network interface provided by the NSD. The VSLAN is currently capable of supporting the following system bus interfaces: IEEE P796 (Multibus-I), DEC Q22, IBM PCXT and PC AT, IEEE P1014/D1.2 (VME), IEEE 1196 (NuBus), and the AT&T 3B2.

The VSLAN mediates access between hosts and datagrams. Its security policy supports both discretionary and mandatory access controls. The discretionary access control (DAC) policy allows two VSLAN subjects to exchange datagrams only if the security officer has authorized communication between them. The mandatory access control (MAC) policy mediates access between VSLAN subjects and datagrams. Each datagram must have associated with it a host-supplied sensitivity label indicating its security level. The VSLAN provides a flexible labeling scheme that supports up to 16 hierarchical classification levels and 64 non-hierarchical categories.

The VSLAN uses the Data Encryption Standard (DES) to encrypt all data transfers across the network. It uses DES primarily as a data integrity mechanism, instead of as a mechanism to enforce the VSLAN security policy. The class B2 MDIA evaluation

criteria does not require the evaluation of the DES; therefore, neither the DES algorithm nor the VSLAN implementation of the DES are evaluated. The hardware and software components that make up the VSLAN, including the LAN cable, must be protected to the highest classification of data processed by the VSLAN. The VSLAN is trusted to protect information at two hierarchically adjacent security classifications. In addition to application environments involving the protection of classified information, the VSLAN could be used to protect unclassified and unclassified-but-sensitive information, which may include financial, proprietary, private, and mission-sensitive data.

EVALUATION SUMMARY:

The security protection provided by the VSLAN has been evaluated by the National Computer Security Center (NCSC) against the requirements specified by the "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria" (TNI), 31 July 1987, NCSC-TG-005, Version 1.

The NCSC evaluation team has determined that the highest class for which the VSLAN satisfies all the specified requirements of the TNI is a class B2 MDIA network component. A class B2 MDIA network component fulfills all the requirements as stated in Appendix A of the TNI for a class B2 Mandatory Access Control component, a class C2 Discretionary Access Control component, a class C2 Identification & Authentication component, and a class C2 Audit component.

The VSLAN covert channel analysis is applicable only to the VSLAN NTCB partition. While it is possible to include an evaluated network M-component such as the VSLAN as part of a network system incorporating other M-components (such as multilevel hosts), this may introduce new covert channels or penetration scenarios that were not evident from the evaluation of either component by itself. A complete network system must always be evaluated as a whole to ensure that the components together enforce the overall policy.

In addition to the network component rating, the NCSC evaluation team has determined that the VSLAN satisfies the requirements for some of the security services described in Part II of the TNI. The services which are offered by the VSLAN are Authentication, Communications Field Integrity, Continuity of Operations, Protocol Based Protection Mechanisms, Network Management, and Data Confidentiality.

The Trusted Computer System Evaluation Summary Chart indicates the requirements and corresponding level that the VSLAN satisfies.

Serial No: CSC/EPL/90/001.A

EVALUATED PRODUCT: VSLAN 5.1 / VSLANE 5.1

VENDOR: Verdix Corporation

EVALUATION DATE: 11 January 1994

OVERALL EVALUATION CLASS: B2 MDIA Network Component

PRODUCT DESCRIPTION:

The Verdix Secure Local Area Network (VSLAN) and the Verdix Secure Local Area Network Exportable (VSLANE) are each a network component that is capable of interconnecting host systems operating at different ranges of security levels allowing a multi-level secure (MLS) LAN operation. The VSLAN/VSLANE is not intended to be a network system. It can be used to build and support a class B2 network system when included in the proper network system architecture. The VSLAN/VSLANE operates at the physical and data-link protocol layers of the Open Systems Interconnection (OSI) reference model, independently of higher-layer, host-to-host protocols. Because of the VSLAN/VSLANE's independence of these upper layer protocols, it can be used to integrate a variety of host systems ranging from DoD internet gateways to vendor-specific systems.

The VSLAN/VSLANE consists of a single Network Security Center (NSC) and up to 128 Network Security Devices (NSDs) interconnected by a transmission medium (i.e., coaxial cable). The NSC is a dedicated computer system that provides a centralized management facility. The NSC supports separate administrator and operator roles. It provides a menu-driven interface for the security officer (i.e., administrator and/or operator) to control the operation of the VSLAN/VSLANE and to collect and store audit data.

Each NSD operates as an individual node of the VSLAN/VSLANE, providing a trusted network interface for its attached host that provides the LAN communications (IEEE 802.3) and enforces the VSLAN/VSLANE security policy for all host-to-host data transfers. Each NSD provides a system bus interface to its attached host and acts as a memory device on its host bus. In order to integrate the NSD with the host operating system, host-specific software is needed to make use of the trusted network interface provided by the NSD. The VSLAN/VSLANE is currently capable of supporting the following system bus interfaces: IEEE P796 (Multibus-I), DEC Q22, IBM PC XT and PC AT, IEEE P1014/D1.2 (VME), IEEE 1196 (NuBus), AT&T 3B2, SBus, MCAe Bus, and the SCSI Bus.

The VSLAN/VSLANE mediates access between hosts and datagrams. Its security policy supports both discretionary and mandatory access controls. The discretionary access control (DAC) policy allows two VSLAN/VSLANE subjects to exchange datagrams only if the security officer has authorized communication between them. The mandatory access control (MAC) policy mediates access between

VSLAN/VSLANE subjects and datagrams. Each datagram must have associated with it a host-supplied sensitivity label indicating its security level. The VSLAN/VSLANE provides a flexible labeling scheme that supports up to 16 hierarchical classification levels and 64 non-hierarchical categories.

The VSLANE uses the Data Encryption Standard (DES) to encrypt all control information on the network. The VSLAN uses the Data Encryption Standard (DES) to encrypt all data transfers across the network. Each uses DES primarily as a data integrity mechanism, instead of as a mechanism to enforce the VSLAN/VSLANE security policy. The class B2 MDIA evaluation criteria does not require the evaluation of the DES; therefore, neither the DES algorithm nor the VSLAN/VSLANE implementation of the DES are evaluated. The hardware and software components that make up the VSLAN/VSLANE, including the LAN cable, must be protected to the highest classification of data processed by the VSLAN/VSLANE. The VSLAN/VSLANE is trusted to protect information at two hierarchically adjacent security classifications. In addition to application environments involving the protection of classified information, the VSLAN could be used to protect unclassified and unclassified-but-sensitive information, which may include financial, proprietary, private, and mission-sensitive data.

EVALUATION SUMMARY:

The security protection provided by the VSLAN/VSLANE has been evaluated by the National Computer Security Center (NCSC) against the requirements specified by the "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria" (TNI), 31 July 1987, NCSC-TG-005, Version 1.

The NCSC evaluation team has determined that the highest class for which the VSLAN/VSLANE satisfies all the specified requirements of the TNI is a class B2 MDIA network component. A class B2 MDIA network component fulfills all the requirements as stated in Appendix A of the TNI for a class B2 Mandatory Access Control component, a class C2 Discretionary Access Control component, a class C2 Identification & Authentication component, and a class C2 Audit component.

The VSLAN/VSLANE covert channel analysis is applicable only to the VSLAN/VSLANE NTCB partition. While it is possible to include an evaluated network M-component such as the VSLAN/VSLANE as part of a network system incorporating other M-components (such as multilevel hosts), this may introduce new covert channels or penetration scenarios that were not evident from the evaluation of either component by itself. A complete network system must always be evaluated as a whole to ensure that the components together enforce the overall policy.

In addition to the network component rating, the NCSC evaluation team has determined that the VSLAN/VSLANE satisfies the requirements for some of the security services described in Part II of the TNI. The services which are offered by the VSLANE are Authentication, Communications Field Integrity, Continuity of Operations, Protocol Based Protection Mechanisms, and Network Management. The VSLAN offers these, as well as Data Confidentiality.

The Trusted Computer System Evaluation Summary Chart indicates the requirements and corresponding level that the VSLAN/VSLANE satisfies.

Serial No. CSC-EPL-94/007

EVALUATED PRODUCT: WATCHDOG

VENDOR: Fischer International Systems Corporation

VERSION: Watchdog PC Data Security version 7.0.2
Watchdog Armor version 1.2.1

EVALUATION DATE: 28 February 1994

OVERALL EVALUATION CLASS: I&A / D2
DAC / D2
AUD / D2
OR / D2

PRODUCT DESCRIPTION:

Watchdog is a combination of three products provided by Fischer International Systems Corporation. Watchdog PC Data Security version 7.0.2 is a software package, while Watchdog Armor version 1.2.1 is a small plug-in hardware board. Also included is Watchdog SecurID, an optional credit card sized authentication mechanism. This product operates on a IBM PC, PC/XT, or PC/AT microcomputer with a minimum of 512K RAM operating under MS-DOS or PC DOS versions 3.0 or higher or IBM OS/2 1.1 standard and 1.1 extended. It also requires at least 2MB of free hard disk space

Watchdog adds Identification and Authentication (I&A), Discretionary Access Control (DAC), Audit (AUD), and Object Reuse (OR) features to the DOS operating system.

EVALUATION SUMMARY:

The National Computer Security Center (NCSC) evaluated the security protection provided by Watchdog against the requirements specified by the Computer Security Subsystem Interpretation (CSSI) of the DoD Trusted Computer System Evaluation Criteria dated September 1988.

An I&A subsystem requires users to identify themselves to it before they do anything on the system. A subsystem rated as an I&A/D2 system must provide a unique identifier and authenticator for each user. Additionally, it must use those items to control access to the protected system, export user identification to the protected system (host), and must provide an auditing mechanism to log security relevant I&A events. Watchdog does provide individual user I&A and an event log and exports user identification to the host. Therefore Watchdog has received an I&A/D2 rating. This evaluation included an optional authentication mechanism called Watchdog SecurID. This provides an additional layer of security to the I&A subsystem. This product is not required for Watchdog to meet the D2 rating for I&A. Both WatchDog PC Data Security software version 7.0.2 and Watchdog Armor version 1.2.1 already satisfy the D2 requirement for an I&A subsystem.

A DAC subsystem provides user-specified, controlled sharing of resources. Security policies establish the rules which determine whether access can be granted. Watchdog meets all of these requirements, and has received a DAC/D2 rating.

An auditing subsystem must be capable of recording all security relevant actions. An audit subsystem with D2 features must be able to integrate into the mechanisms that mediate access and perform user I&A. It must always be invoked, and must be tamper proof. Watchdog records all security relevant actions and interfaces with the I&A and DAC mechanisms. Therefore Watchdog has received an AUD/D2 rating.

An Object Reuse subsystem must clear storage objects to prevent subjects from scavenging data from storage objects which have been previously used. Watchdog overwrites file system objects upon deallocation, and clears all memory objects at the end of a user's session., satisfying the D2 requirement for Object Reuse.

For a complete description of how Watchdog satisfies each requirement of the CSSI, see Final Evaluation Report, Fischer International Systems Corporation Watchdog Version 7.0.2 (Report no. CSC-EPL-94/007).

Serial No.CSC-EPL-92/00

EVALUATED PRODUCT: XTS-200 STOP 3.1.E

VENDOR: HFSI

VERSION EVALUATED: STOP 3.1.E

EVALUATION DATE: 27 May 1992

OVERALL EVALUATION CLASS: B3

PRODUCT DESCRIPTION:

The XTS-200 system runs on the Bull HN Information Systems Inc. DPS 6 PLUS and DPS 6000. STOP is a multilevel secure operating system that runs on the XTS-200 hardware. XTS-200 refers to the combination of STOP and the hardware which includes the DPS6 PLUS and DPS 6000-400/500/600 families. The XTS-200 is a multiprocessor system capable of supporting up to four independent processors. It implements a virtual memory of up to two gigabytes, and a ring mechanism for protection. STOP is a multiprogramming system which can support up to 256 users. It supports much of the UNIX System V interface for applications software.

STOP consists of four components: the Security Kernel, which operates in the most privileged ring and provides all mandatory, and a portion of the discretionary, access control; the Trusted Computing Base (TCB) System Services, which operates in the next-most-privileged ring, and implements a hierarchical file system, supports user I/O, and implements the remaining discretionary access control; Trusted Software, which provide the remaining security services and user commands; and Commodity Application Services System (CASS), which operates in a less privileged ring and provides the UNIX-like interface. CASS is not in the TCB.

The XTS-200 uses the DPS 6 PLUS and DPS 6000 hardware. The DPS 6000 hardware uses Bull firmware. The DPS 6 PLUS hardware uses Bull firmware with modifications developed by HFSI. STOP was developed by HFSI. XTS-200 is marketed and supported by HFSI. STOP 3.1.E was released in May 1992.

The system provides mandatory and discretionary access control which allows for both a secrecy and integrity policy. The mandatory security policy enforced by the XTS-200 is based on the Bell and LaPadula security model; the mandatory integrity policy is based on the Biba integrity model. The system provides for user identification and authentication used for policy enforcement through user IDs and passwords, and individual accountability through its auditing capability. Data scavenging is prevented through object reuse. The trusted path mechanism is provided by the implementation of a Secure Attention Key (SAK).

The separation of administrator and operator roles is enforced using the integrity policy. The system enforces the "principle of least privilege" (i.e., users should have no more authorization than what is required to perform their functions) for each of the two defined privileged roles available. All actions performed by privileged users can be audited. The audit log is protected from modification. STOP also provides an alarm

mechanism to detect the accumulation of events that indicate an imminent violation of the security policy.

The TCB has been analyzed and found to meet the minimization requirement which reduces complexity and to meet the layering, abstraction, and data hiding requirement. The TCB has been tested thoroughly and has been found to be resistant to penetration. The system developer has also provided a model and a descriptive top-level specification on which the design of the TCB is based.

EVALUATION SUMMARY:

The security protection provided by XTS-200, when configured in a secure manner as described in the Trusted Facility Manual, has been evaluated by the National Security Agency (NSA) against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria [DOD 5200.28-STD] dated December 1985.

The NSA evaluation team has determined that the highest class at which XTS-200 satisfies all the specified requirements of the Criteria is class B3. For a complete description of how XTS-200 satisfies each requirement of the Criteria, see Final Evaluation Report, HFSI XTS-200 (Report CSC-EPL-92/003).

In addition, the report should also be consulted for the complete lists of evaluated hardware and software components.

APPENDIX C
OTHER SECURITY PRODUCTS

ASSESSED PRODUCT: Access Managed Environment

VERSION: 2.1

VENDOR: Casdy & Greene, Incorporated

FINAL ASSESSMENT REPORT: 92-510 30 September 1993

PRODUCT DESCRIPTION:

Access Managed Environment (AME) 2.1 by Casady and Greene, Incorporated(C&G), is a
product for Macintosh computers running the System 7 operating system. Its features include password protection, discretionary access control, virus protection, and an audit log.

ASSESSMENT SUMMARY:

Product performance was checked against vendor claims, with emphasis placed on checking for hard disk writes by users without that privilege. Password protection was easily circumvented granting the user limited access to the harddisk (HD). Floppy disks inserted at the sign-on screen could be accessed even if a user lacked floppy disks privileges. Software on floppy disks registered to AME could be used by any user, even if he were forbidden access to the same software on the HD. The audit log recorded neither multiple attempts to access forbidden files nor multiple failed attempts to sign on, thus making it impossible to tell accidents from deliberate hacks. The system clock could be changed by any level of user, making it easy to fool the audit log. The audit log did not record any activity if the sign-on screen were bypassed. Names of files and occasionally (if clipboard memory became too small) file data were written to the HD even when the user lacked privileges to write to the HD. Users without privileges to write to the HD could still record sounds and take a "snapshot" of the "desktop," i.e., create a MacDraw file saved to the HD containing a picture of the screen.

ASSESSED PRODUCT: Certus

VERSION: 2.1

VENDOR: Certus International Corporation

FINAL ASSESSMENT REPORT: 92-504 15 November 1992

PRODUCT DESCRIPTION:

Certus Version 2.1 is designed to safeguard designated programs and provide a more secure computing environment for disk operating system (DOS) based personal computers (PCs) for both stand-alone and networked modes. This assessment only focuses on the stand-alone mode.

When Certus is properly installed on a machine, it sits in the background transparent to the users. Certus acts as an extension to DOS. Certus makes the following security claims: Protection against any unknown program being run on the system; disabling access to the hard drive when booted from floppy; protection of system critical files (i.e., autoexec.bat); some discretionary access controls; protection against software theft; software usage logs; and an overwrite function.

ASSESSMEMT SUMMARY:

While Certus does meet most of its functional claims, in many areas Certus falls short of meeting national criteria as described below, and some vulnerabilities exist to malicious attacks. Certus' best attribute is the ability of the system manager to strictly control which programs can be run on the system. At security level 1, no program can be run without first being added to the approved file signature list. Certus is also successful in preventing any circumvention of the autoexec.bat file by disabling keyboard interrupts until Certus is fully loaded into memory. Certus also checks for any alteration of system critical files upon boot up as well as requiring a password for the completion of the boot up sequence.

Contrary to the documentation, Certus does have many vulnerabilities. The bootlock function was able to prevent a user from accessing the hard drive from the command line; however, it is possible to circumvent this function using a simple disk editing utility. It is then possible to edit the autoexec.bat file and disable all Certus files which execute at start-up. Another vulnerability of the system is that the password used at start-up is stored in the clear text of the random access memory (RAM). Therefore the password is accessible by using a RAM viewing utility program. The overwrite function is compliant with the national criteria outlined in A Guide To Understanding Data Remanence in Automated Information Systems except for the fact that the file name is not deleted from the directory. It is also important to take into account that this program does not overwrite the backup file created by some word processing programs.

We recommend that to maximize the advantages of Certus, no RAM viewing program should be allowed on the system. A malicious user would then not be able to use this function because it would not be in the approved file list.For maximum security the security level should always be set to one and the floppy drives should be physically

disabled. If the floppy drives are not disabled, it will always be possible to bypass the Certus security features.Regardless of whether the floppy drives are disabled, Certus' bootlock program should be used with the password set to General User. This will ensure that anyone using the system will have to know the password, but they will not be able to access any of the administrator functions. Certus recommendations should also be followed for protecting system critical files.

ASSESSED PRODUCT: Computer Security Toolbox Version 1.7

VENDOR:

FINAL ASSESSMENT REPORT: 93-503 21 April 1993

PRODUCT DESCRIPTION:

The Computer Security Toolbox Version 1.7 programs are the cooperative effort of several elements of the Intelligence Community. The Computer Security Toolbox was compiled by the Air Force Intelligence Command (AFIC) and consists of programs written by the Naval Security Group (NSG), the National Security Agency (NSA), International Business Machine (IBM) Corporation, and by AFIC itself. The Computer Security Toolbox contains five programs: TOOLBOX, SCOPY, FLUSH, BUSTER, and VIRSCAN.

The Computer Security Toolbox provides Object Reuse (overwrite) in the FLUSH program.

NOTE: The VIRSCAN, written by IBM, was not assessed by the PACC. The product was assessed previously by AFCSC (Project 92-700, 1 June 1992).

ASSESSMENT SUMMARY:

Although the Computer Security Toolbox Version 1.7 programs were considered to be a security subsystem rather than a complete trusted computer system, it was assessed against the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. In addition, the FLUSH program was assessed against the overwrite procedures outlined in the Air Force Systems Security Instruction Remanence Security (AFSSI-5020), 15 April 1991.

BUSTER was considered to have major problems because it does not provide adequate protection on the test configurations.

FLUSH was found to function as stated in the vendors' product description documentation. However, this overwrite procedure DOES NOT overwrite hidden or read-only files and BAD disk sectors. In addition, this overwrite procedure DOES NOT meet the government standards for PURGING of data disks as per AFSSI-5020.

SCOPY was found to function as stated in the vendors' documentation. When the FLUSH and SCOPY programs were used in conjunction with dBase III PLUS .DBFfiles, they DID NOT overwrite the file slack or copy effectively because of the limitations of the dBase III PLUS program. However, when these programs were used in conjunction with Foxbase 2.0 and FoxPro 2.0, they DID overwrite the file slack and copy effectively.

ASSESSED PRODUCT: Security Guardian

VERSION: 3.63

VENDOR: COMMAND Software Systems, Incorporated

FINAL ASSESSMENT REPORT: 92-507 22 June 1993

PRODUCT DESCRIPTION:

Security Guardian is a software package that provides security protection of sensitive data on a personal computer (PC). The front end security, a Boot Protection mechanism, prevents unauthorized access to hard disk(s). Booting from the floppy disk and then attempting to access any hard disk returns the message "Invalid Drive Specification." Security Guardian is designed to protect all hard disks, physical as well as logical.

Some of the security functions provided by Security Guardian are:Identification and Authentication (I&A), Discretionary Access Control (DAC),Object Reuse, and Audit.

ASSESSMENT SUMMARY:

Although Security Guardian (Version 3.63) programs were considered to be a security subsystem rather than a complete trusted computer system, they were assessed against the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The security features included I&A, DAC, Object Reuse, and Audit. In addition, the CSS Wipe(overwrite) program of Security Guardian was assessed against the overwrite procedures outlined in the Air Force Systems Security Instruction (AFSSI-5020)Remanence Security, 15 April 1991.

Security Guardian and its options were found to function as stated in the vendors' documentation.

The following security mechanism functioned as stated in the vendors' documentation. However, because the Boot Protection mechanism could be defeated by altering its configuration, it DOES NOT provide adequate protection on the test configurations listed in para 5.1:

Boot Protection

The following security mechanism was found to function as stated in the vendors' documentation. However, because various disk utility programs verified the presence of unencrypted passwords in memory, it DOES NOT provide adequate protection:

Identification and Authentication

The following security mechanism was found to function as stated in the vendors' documentation. However, the government overwrite specifications as outlined in AFSSI-5020 could not be verified:

Object Reuse

The following security mechanism was found to function as stated in the vendors' documentation. However, the audit files were not updated when the hard disk became full. This DOES NOT meet the requirements of the TCSEC:

Audit

The following security mechanism was found to function as stated in the vendors' documentation and met the requirements of the TCSEC:

DAC

ASSESSED PRODUCT: Security Guardian

VERSION: 3.7

VENDOR: COMMAND Software Systems, Incorporated

FINAL ASSESSMENT REPORT: 93-505 31 August 1993

PRODUCT DESCRIPTION:

Security Guardian is a software package that provides security protection of sensitive data on a personal computer (PC). The front end security, a Boot Protection mechanism, prevents unauthorized access to hard disk(s). Booting from the floppy disk and then attempting to access any hard disk returns the message "Invalid Drive Specification." Security Guardian is designed to protect all hard disks, physical as well as logical.

Some of the security functions provided by Security Guardian are:Identification and Authentication (I&A), Discretionary Access Control (DAC),Object Reuse, and Audit.

ASSESSMENT SUMMARY:

Security Guardian (Version 3.7) programs were considered to be a security subsystem rather than a complete trusted computer system, they were assessed against the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The security features included I&A, DAC, Object Reuse, and Audit. In addition, the CSS Wipe(overwrite) program of Security Guardian was assessed against the overwrite procedures outlined in the Air Force Systems Security Instruction (AFSSI-5020)Remanence Security, 15 April 1991.

Security Guardian and its options were found to function as stated in the vendor's documentation.

The following security mechanism functioned as stated in the vendor's documentation. However, it DOES NOT provide adequate protection on the test configurations listed in para 5.1. In addition, this mechanism can be completely bypassed using the F5 or the F8 keys in MS-DOS 6.0:

Boot Protection

The following security mechanism was found to function as stated in the vendor's documentation. However, the overwrite specifications as outlined in AFSSI-5020 could not be verified:

Object Reuse

The following security mechanisms were found to function as stated in the vendor's documentation:

I&A

DAC

Audit

ASSESSED PRODUCT: TOVEN Secure Notebook

VERSION: N/A

VENDOR: TOVEN

FINAL ASSESSMENT REPORT: 93-507 20 January 1994

PRODUCT DESCRIPTION:

The TOVEN Secure Notebook uses a Notepro Series Notebook Computer with a 120 MB non-removable hard disk. Security is provided by independent hardware. The notebook will not activate without a smart card being inserted and the correct password entered. All information stored on the hard disk is encrypted using DES cypher block encryption. When a smart card is inserted into the unit,the correct password given, the encryption keys for the hard disk are loaded from the smart card into the security module. These keys can then be used to decrypt/encrypt information as it is read/written from or to the hard disk. When the smart card is removed from the unit, the encryption keys in the TOKEN security module are erased and the system is forced to shut down.

ASSESSMENT SUMMARY:

The TOVEN Secure Notebook was assessed under the Computer Security Subsystem evaluation program. Although this program was considered to be a security subsystem rather than a complete trusted computer system, it was assessed against the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), 26 December 1985. The security features included Identification and Authentication (I&A) and Discretionary Access Control (DAC).

The TOVEN Secure Notebook performed as advertised and is fully functional with its stated design purposes.

RECOMMENDATIONS:

Recommend that the TOVEN Secure Notebook not be used to process classified information. At present, there is no way to overwrite the internal hard disk. The only other means would be to degauss the hard disk. Recommend that the System Administrator (SA), when installing Windows applications, exercises extreme care because of the compatibility problem inherent with the TOVEN Secure Notebook encryption scheme. Recommend that the TOVEN Secure Notebook incorporate in its security module a configuration to enforce password updates based on a minimum and maximum password lifetime as defined by the SA. Recommend an auto log feature be incorporated. This would protect the user's information without requiring an exit from the current application. This feature would be automatically invoked after a fixed period of inactivity.

ORIGINAL EVALUATED PRODUCT: SVS/OS CAP 1.00

VENDOR: Wang Laboratories, Inc.

RATING MAINTENANCE DATE: 16 September 1991

OVERALL EVALUATION CLASS: C2

EVALUATION SUMMARY:

Wang Laboratories, Inc. has maintained the C2 rating of its Virtual Operating System with Controlled Access Protection, through participating in RAMP. VS/OS CAP 1.01 is a maintenance release of VS/OS CAP 1.0 which was formally evaluated at C2. There have been no intervening product releases. The changes in VS/OS CAP 1.01 have been designed and analyzed in accordance with National Security Agency's Ratings Maintenance Program.

PRODUCT DESCRIPTION:

Wang's Secure Virtual Storage Operating System with Controlled Access Protection, SVS/OS CAP 1.01, runs on the Wang VS Product Family, a series of 32-bit super-minicomputers with a virtual memory system that can support from 512KB to 32MB of addressable physical storage. SVS/OSCAP 1.01 consists of the VS Operating System, release 7.33.36 Enhanced Security Access Controls (ESAC), and I/O Device Support Package Version 5.0.

SVS/OS CAP 1.01 is a general-purpose time-sharing system which supports identification and authentication of users, discretionary access controls, object reuse protection, and auditing.

SVS/OS CAP 1.01 provides isolation of the TCB from users. Process isolation is implemented through the use of individual process virtual address spaces and hardware memory protection mechanisms.

User accounts are maintained in a protected system file by the System Administrator. Each account has a logon ID and a password. SVS/OS CAP1.01 also provides optional password control capabilities which include system generated passwords; password expiration; limiting of invalid logon attempts; locking of unused logon IDs; restricting logons for a logon ID by time and date; enforcing minimum password length;maintaining a password history to prevent the reuse; and password encryption.

Discretionary access controls (DAC) on files consist of access control lists and file protection classes which use hierarchical access levels(Write, Read, Execute, and Null). The access control lists can allow access by, or deny access to, individuals or groups of individuals.

SVS/OS CAP 1.01 provides auditability of all security-relevant events.The SA can select events to be audited, create log files, and specify log file sizes. The selectivity of events is based on three categories:system, file, and user. System events are the events auditable for every file and user on the system. File events are the auditable events related to a particular file, or set of files, and user events are the events auditable for a given user ID or set of user ID, including operators. The SA is able to select events to be audited through a menu driven interface. SVS/OS CAP 1.01 allows the SA to produce reports based upon the audit data. These reports are easy to read and interpret.