SECURITY FUNCTIONALITY REQUIREMENTS

National Institute of Standards and Technology

Gaithersburg, MD

MINIMUM

SECURITY FUNCTIONALITY REQUIREMENTS

FOR

MULTI-USER OPERATING SYSTEMS

Issue 1

January 28, 1992

- Computer Security Division
- Computer Systems Laboratory
- National Institute of Standards and Technology
- A Preliminary Contribution
- to the New
- "Federal Criteria"

--

- Federal Information Processing Standard
- on
- Trusted Systems Technology

NOTES TO REVIEWERS

This is a draft of work in progress by the Minimum Security Requirements (MSR) Working Group of the Joint NIST-NSA Federal Criteria (FC) Project. It is provided for preliminary review and comment by members of the international computer security community. The Minimum Security Functionality Requirements (MSFR) contained herein are designed to become a part of the new Federal Information Processing Standard (FIPS) on Trusted Systems Technology under development by the FC Project. That FC-FIPS is expected to replace the Trusted Computer System Evaluation Criteria (TCSEC) or "Orange Book."

Our objectives in presenting this MSFR material now in its incomplete form are twofold: first, to give the community an early view of the FC Project's direction in moving beyond the TCSEC method of expressing requirements; and second, to obtain feedback on the scope and content of the proposed minimum functionality requirements, the method of their presentation, and their granularity. These requirements are expected to form the foundation for all requirements classes in the FC-FIPS.

The MSR Working Group has been tasked to develop a new requirements class to replace C2. This new class is to be oriented heavily towards common non-classified government and commercial minimum security requirements for multi-user operating systems. This requirements class is to be significantly updated from C2 and must include clearer directions to computer vendors by incorporating greater detail while still permitting innovation. The working group has concentrated first on developing the new functionality portion of the requirements, contained in this document. The companion minimum assurance requirements are still under development and are not ready for public review. It is planned that they will be based on common assurance requirements for C2 in the TCSEC and for the E2 level in the Information Technology Security Evaluation Criteria (ITSEC), version 1.2.

The Working Group is adopting the format of an ITSEC Security Target for expressing the new minimum requirements class. Please note that we consider the Product Rationale Section of the Security Target included here to be very incomplete at this point. No worked examples of ITSEC-style Security Targets are yet available as guides. Reviewers are especially encouraged to provide input to the Product Rationale Section.

As a preliminary draft of one portion of the new FC-FIPS, this document is not intended for general distribution or compliance.

- The document should not be considered to be a complete or finished product. Your comments will be used by the MSR Working Group to help raise the maturity level of this material before it is included in the new draft FC-FIPS

1. INTRODUCTION

- A proposed minimum set of security functionality requirements for general purpose multi-user operating systems is presented. This set implies the existence of a companion set of minimum assurance requirements, especially those relating to vendor development life-cycle assurance. The functionality requirements are based on the Trusted Computer System Evaluation Criteria (TCSEC) [1] C2 requirements class, with additions from current computer industry practice and commercial security requirements specifications. It is anticipated that the companion assurance requirements, when completed, will meet both the TCSEC's C2 requirements and the Information Technology

Security Evaluation Criteria (ITSEC) [2] level E2 requirements. This document has been organized to fit the Security Target template described in ITSEC Sections 2.3 to 2.58.

1.1 Federal Criteria

- The requirements contained in this document have been developed as part of a joint National Institute of Standards and Technology (NIST) and National Security Agency (NSA) project to produce a Federal Information Processing Standard (FIPS) that will ultimately replace the TCSEC. That effort is called the Federal Criteria (FC) Project. These requirements have been developed by the Minimum Security Requirements (MSR) Working Group of the FC Project under NIST leadership with a high level of private sector participation. The requirements developed by that group and contained temporarily in this document can be viewed as an enhanced replacement for C2, to be contained in the new FC-FIPS. Another FC Project Working Group is addressing the higher levels of security.
- The NIST/NSA FC Project envisions development over the next few years of a series of FIPS and other documents that will provide criteria and guidance on security in operating systems and other information technology (IT) areas such as networks, data bases, and applications. The FC-FIPS are intended to serve a number of purposes, similar to those of the TCSEC. They are intended to be useful to a broad base of users including the private, civil government, and national defense communities. Recognizing that IT product vendors operate in an international marketplace, these criteria will be built to complement international efforts, such as the ITSEC and International Standards Organization (ISO) initiatives.

1.2 Background

- Government and commercial institutions rely heavily on information processing systems to meet their individual operational, financial, and informational requirements. The integrity, availability, and confidentiality of key software systems, databases, and data networks are major concerns throughout all sectors. The corruption or unauthorized disclosure or theft of corporate resources could have a disruptive effect on the continuity of an organization's operations as well as serious and immediate financial, legal, and public confidence impact.

1.2.1 TCSEC

- The US government has been involved in developing security technology for computer and communications systems for some time. The TCSEC was originally published in 1983 and revised in 1985. The TCSEC represents the

culmination of many years of effort to address IT security issues within the Department of Defense (DoD) classified world. Since its publication, the TCSEC has influenced vendors, consumers, and the authors of other requirements documents both in the US and abroad. The impact of the TCSEC on the field of IT security is widely recognized. It has helped form the foundation for the development of these second-generation requirements.

- Although the contributions of the TCSEC have been great, it does not completely address the IT-oriented security needs of organizations handling non-classified information. The TCSEC is made up of IT security features and assurances which have been derived and engineered to support a very specific DoD security policy. The TCSEC was created to meet one major security objective-prevention of unauthorized disclosure or "leakage" of classified information. Organizations outside the DoD classified world do not necessarily have this policy as their most important security objective. Commonly, they tend to view a combination of data integrity and system availability as more important than confidentiality.
- Until recently, little comparable attention has been paid to researching and addressing the IT security needs of the non-classified government (both civil and military) and private sectors. During the past few years, however, the managers and security officers of commercial and non-classified government enterprises have paid increasing attention to IT security needs. TCSEC-motivated security features have proven valuable in helping solve security problems outside of the DoD classified world. Yet, often these features are viewed as less than perfect and incomplete, and they are specified in the absence of a more appropriate set of security functions.

1.2.2 ITSEC

- In June of 1991, the European Community adopted the ITSEC version 1.2 for a trial period of two years. The ITSEC represents a harmonized effort among France, Germany, the Netherlands, and the United Kingdom that builds on various national initiatives, including the TCSEC. The ITSEC provides a basis for evaluating any specified set of IT security functionality in terms of correctness and effectiveness. It provides a methodology for gaining confidence in the security functions implemented in IT products and systems by use of a set of well-defined assurance evaluation levels.
- The ITSEC does not specify security functionality requirements but rather permits the definition and use of a variety of functionality profiles. The ITSEC describes an approach called a Security Target for specifying and justifying the security functionality and level of assurance required in a particular product or system.
- As the minimum security functionality requirements contained here may be of value internationally, they are being expressed generally in the format of an ITSEC Security Target. This target, if widely accepted, could help form the basis for mutual recognition between nations of product evaluations.
-

1.3 Scope and Applicability

- These minimum security functionality requirements address general purpose, multi-user operating systems. As such, they must be viewed as "product" and not "system" requirements.
- These requirements are "baseline" requirements in the sense that they comprise minimum security expectations for multi-user operating systems. These requirements apply generally to multi-user workstations, minicomputers, and mainframes. They do not address security requirements that are specific to a particular type of computer system. For example, workstation-specific requirements are not addressed.
- These requirements are not specifically intended for use in the design of a computer network, nor do they address the potentially unique requirements of network components such as packet switches, routers, or front ends. However, they do address network interfaces to the operating system and specify distinct requirements for the identification, authentication, and system access control of remote machines.
- These requirements are not intended to be used for the development or assessment of specific applications. However, they may be used as a basis or a set of guidelines to assist designers in constructing application-specific requirements. Operating system security mechanisms are typically utilized by an application to meet its own security requirements.
- These requirements only cover security features. The security features describe what functionality is required and how that functionality is to be provided. As such, these requirements do not include assurance requirements (which are still under development).
- Product vendor adherence to these requirements does not guarantee a "secure" system. It does not reduce the using organization's responsibility to operate and maintain systems containing these operating system products in a secure fashion. Security is not only the vendor's responsibility but it is also the responsibility of the application software developer who builds upon these operating systems, the operations staff who maintain the total systems in their operating environments, and the ultimate end-user who uses these systems.
- These requirements do not address physical security, personnel security, disaster recovery plans, or other security issues specific to environment and usage, which are almost always required in addition to effective use of the product's security features.
- These requirements do not dictate site-specific administrative policies and procedures. However, they do require that an operating system vendor provide the features and mechanisms necessary to implement a reasonable site-specific security policy. The vendor is also required to provide documentation on how to use these mechanisms effectively to implement such a policy.
-

1.4 Sources of Minimum Requirements

- These requirements in large measure reflect common practices and proven technology for protecting computer resources from unauthorized use. They were based on information gathered about the needs of many computer system users in private, civil government, and defense organizations. As such, they are based on a number of sources. The most important of these are:
  - 1. The TCSEC C2 requirements.
  - 2. The National Research Council's "Computers at Risk, Safe Computing in the Information Age" [4].
  - 3. "Bellcore Standard Operating Environment Security Requirements" [7], written by Bellcore. The author of this document is a member of the MSR Working Group
  - 4. "Commercial International Security Requirements" [6], written by American Express and Electronic Data Systems. The principal author of this document is an adjunct member of the MSR Working Group.
  - 5. Draft NIST report "Assessing Federal and Commercial Information Security Needs" [3], December 6, 1991 (described below). The principal author of this document is a member of the MSR Working Group.

As the first step toward developing a comprehensive FIPS, NIST conducted a survey in 1991 to assess the information security requirements of key elements of thirty important U.S. organizations, including Federal agencies, commercial enterprises, and state governments. The minimum security functionality requirements contained in this document were strongly influenced by the formal and informal observations made by NIST researchers during the survey. The results of the survey were contained in the draft NIST report listed above. That report, to be published in early 1992, determined:

- 1. There is a need to move beyond confidentiality and address integrity and reliability requirements.
- 2. Strong identification and authentication methods are needed.
- 3. A method for administratively-imposed access controls based on user role or job responsibility must be developed. However, this topic demands further research and is not addressed in the present set of requirements.
- 4. The security administrator's interface, which is a critical component in controlling access to information, must be easy to use.

1.5 Target Audiences

- These requirements are targeted at three distinct audiences: users, vendors, and evaluators.

Users

This set of minimum security functionality requirements addresses the basic security needs of general-purpose computer operating systems users. This includes application developers, end users, and administrators in the private, civil

government, and defense sectors. The requirements focus on the minimum level of security that should be a part of any commercially available multi-user operating system. All functionality requirements are based on existing and well understood security practices. Specific user communities could build on these minimum requirements by adding their own environment or application specific requirements. When included in the new FC-FIPS, this set of security functionality requirements will set a minimum level of expectation within the user community about the security of the operating system products they purchase. It is anticipated that vendors will respond to user expectations by increasing the availability of operating systems products that meet these minimum security requirements.

Vendors

Vendors will be provided with a single, well-defined set of minimum security functionality requirements that can be accepted across their entire non-classified customer base. These requirements have been composed with input and cooperation from government standards and security organizations, major commercial end-users and software developers, as well as hardware and operating system vendors. These requirements represent the harmonization of a number of security requirement specifications from various sources into a single set that has potential for very wide acceptance. Vendors can more confidently use this set to focus on a single product offering, thus decreasing development and support costs and allowing more directed marketing efforts. The level of detail used here should help clarify what the vendor must do to comply. It should also permit narrower latitude for evaluator subjectivity. However, vendors would still have the flexibility to use new approaches meeting the basic security objectives.

Evaluators

Product and system evaluators, certifiers, and accreditors are provided with a well-defined and unambiguous set of minimum security functionality requirements. The detailed level of the requirements significantly decreases the need for evaluator interpretation. The organization of the rationale and functions in ITSEC Security Target format is aimed at providing a basis for international acceptance that can help lead to mutual recognition of evaluations.

1.6 Evaluation of Products

- As part of the FC Project, NIST and NSA are planning to broaden the trusted product evaluation program substantially by accrediting laboratories to evaluate commercially-oriented products. This new program will be called the Trust Technology Assessment Program (TTAP) and will be based on the new Federal Criteria. This program will be directed towards the security assessment of products with minimal assurance requirements. The TTAP is being

developed with the three goals of assisting the international recognition of product evaluations, minimizing time and cost of product assessments and maximizing product availability.

1.7 Document Structure

This document is organized into six sections: Introduction, Product Rationale, Specification of Security Enforcing Functions, Other Security Target Requirements, Glossary and References. The Product Rationale, Specification of Security Enforcing Functions, and the companion Minimum Security Assurance Requirements (upon their development) are the principal sections to be merged into the draft FC-FIPS as integral parts. Material in other sections will be used in the FC-FIPS as appropriate.

1.7.1 Product Rationale

The Product Rationale section follows the format of ITSEC Sections 2.16 and 2.17 and is divided into the following headings.

1. Identification of the intended method of use.
2. Identification of the intended environment for use.
3. Definition of all assumptions about the environment and the way in which the product will be used.
4. Identification of assumed threats for that environment.

1.7.2 Specification of Security Enforcing Functions

The Specification of Security Enforcing Functions section generally follows the format of ITSEC Section 2.18, "Specification of Security Enforcing Functions," and Section 2.31, "Generic Headings." It is divided into the following eight sections:

1. Identification and Authentication
2. Access Control
3. Accountability
4. Audit
5. Object Reuse
6. Accuracy
7. Reliability of Service
8. Data Exchange

Each section specifies a high level control objective and a set of detailed security requirements. For any section, the product developer may choose to comply with either the high level control objective or the detailed requirements.

1.7.3 Other Security Target Requirements

- This section contains information addressing the final three requirements for an ITSEC-style Security Target, which include Required Security Mechanisms, Minimum Strength of Mechanism, and Target Level of Evaluation. The latter is due to be replaced with a section called Minimum Security Assurance Requirements, which are being developed.
- These assurance requirements will be included in the draft FC-FIPS when it is circulated for comment. When included, the assurance requirements will follow the format of ITSEC Section 2.26, "Target Level of Evaluation," and will provide appropriate material related to the effectiveness and correctness sections.
-

1.7.4 Glossary

- Definitions in the glossary come from the source documents mentioned above as well as the ISO International Standard 7498-2, "Information Processing Systems - Open Systems Interconnection Reference Model - Part 2: Security Architecture" [8].
-
-

1.8 Terminology

- The following terminology is used throughout this document:
- Requirement: Feature or function that is necessary to satisfy the needs of a typical commercial enterprise or government organization. Failure to meet a Requirement may cause application restrictions, result in improper functioning of the product, or hinder operations. A Requirement contains the word shall and is identified by the letter "R" in parentheses: ®
- Advisory: Feature or function that is desirable and may be required by a typical commercial enterprise or government organization. An Advisory represents a goal to be achieved. An Advisory may be reclassified as a Requirement in future versions of the FC.

2. PRODUCT RATIONALE

- This section follows the format of the Security Target "Product Rationale" in ITSEC Sections 2.16 and 2.17. The generic product rationale given here is used to establish the basis for the "Specification of Security Enforcing Functions" described in Section 3. Those functions are identical to what we call Minimum Security Functionality Requirements (MSFR) for multi-user operating systems.
- This product rationale is applicable to products that are to be designed and built to meet the MSFR. As specified in the ITSEC, this product rationale is based on the combination of the environment in which the product is to be

used, intended use of the product, and assumed threats the product is expected to counter given that environment and usage. It is expected that vendors may need to provide additional rationale information for their individual products if the intended usage and environment are more specific than that provided here.

- However, it should be noted that the MSFR were developed first by a bottom up approach and then later by a top down approach to match the ITSEC. The MSFR are originally based on a wealth of practical experience and observations of actual multi-user operating system usage in a general business environment. In addition to existing C2 requirements, information on useful and practical security features was solicited from a variety of end users, developers and evaluators. The MSFR also follows the top down approach of the ITSEC Product Rationale, in which the expected product environment and usage dictate a set of necessary security enforcing functions to counter anticipated valid threats. As this top-down approach was added in to comply with the ITSEC after the MSFR had already been developed, this version the Product Rationale may not yet be complete.

2.1 Intended Method of Use

- The MSFR addresses general purpose, multi-user operating systems, with the expectation that they will be used in a wide variety of applications. No special constraints are indicated in the usage of these systems. However, they are not specifically intended to be used where information at different levels of sensitivity to disclosure or modification must be protected separately or where user access requirements must be controlled rigorously. Products designed with the MSFR as Security Target are intended for processing a single protection level of information.
- These requirements apply to multi-user workstations, minicomputers, and mainframes. They do not address any security requirements that are specific to a particular type of computer system. For example, workstation-specific requirements are not addressed.

2.2 Intended Environment for Use

- These requirements address general purpose, multi-user operating systems. Products designed against the MSFR will operate in a wide range of environments, typically of a general business nature. No specific constraints are placed on environments for products meeting the MSFR. Environments are expected to include commercial, non-classified military, single-level classified military, and civil government.

2.3 Assumptions About the Environment and Use

- These requirements assume the existence of a routine, well-managed operational environment following ordinary business practices. They make no

expectations about the type of information processed or its attractiveness to attackers. They assume that attackers will have the ability to gain nominal access to the product. It is therefore a user/operator function to determine the need and apply appropriate types of controls in the environment over such nominal access. Similarly, these requirements do not address any specific physical security needs, required personnel security policies, disaster recovery plans, or other environmental security concerns.

2.4 Assumed Threats for That Environment

- Like the TCSEC C2 requirements class, the MSFR was developed principally to mitigate the general threat from "penetration" attempts against systems operating in the types of environment described above. The penetration threat occurs when an attacker who already has nominal access to a system attempts to gain additional access to system resources and data or circumvent the system security policy. A variant of this threat exists when a system user unintentionally performs actions permitting him/her to gain inappropriate access to system resources and data.
- The MSFR and its predecessor C2 requirements were designed as "reasonable first-line defenses," with the understanding that in high-payoff circumstances highly motivated attackers would be willing to apply the level of work effort needed to circumvent them. Under such circumstances, a product designed to meet the MSFR would be inappropriate. It should be noted that a system that has been designed and developed in total compliance with the MSFR can and will contain vulnerabilities to higher levels of attack. This fact is recognized in the stipulation of only a basic level of strength in the Minimum Strength of Mechanisms section of the Security Target.
- The MSFR was not specifically developed to eliminate the threat from malicious software. However, these requirements contribute towards the reduction of threats such as trojan horses and viruses.
- The following sections discuss the expected threats given the above-stated product usage and environment, in the context of the MSFR "Specifications of Security Enforcing Functions" described in Section 3.

2.4.1 Threats Countered by Identification and Authentication

- Identification and authentication requirements of the MSFR promote and support controls that can be used to protect against a variety of threats. Of particular consideration are threats of unauthorized access at the system interface and system resource levels.
- Identification requirements of the MSFR apply to both direct system users and remote machines. Specific requirements address the creation, revoking, grouping and administering of user and system IDs.
- The MSFR focuses on the more common password methods for validation of userIDs but permits a variety of other authentication approaches. These methods include smart-cards, cryptographic-based authentication, and

biometrics, among others. Although such authentication methods may be stronger, passwords continue to be used almost exclusively today. For this reason, detailed requirements for password based systems are specified as part of the MSFR. In addition to their mandatory use at initial system access, authentication mechanisms such as passwords have great value in strengthening and enhancing the access control methods.

- For this reason the MSFR specifies general password facilities for optional use by application programmers, system administrators and end-users for the enhanced protection of system resources such as sensitive files and transactions. Detailed password authentication requirements address the creation, use, and management of passwords. As other authentication approaches such as smart-cards become more prevalent and better understood, a similar level of specificity will be provided for them.

2.4.2 Threats Countered by System and Resource Access Control

- The MSFR specifies access control requirements at both system interface and system resource levels. Such requirements provide protection against unauthorized access and the unauthorized use of system resources. These requirements have the goal of protecting both the privacy and integrity of system resources.
- System access control requirements specify which users, under what conditions, whether locally or remotely connected, can gain access to the protected system. Specified controls are based on userID, time, location, method, access mode and access path. Additional requirements specify keyboard locking, failed logon attempt management, as well as advisory and warning message.
- At a system resource level, the MSFR specifies access control features to mediate user access to data, as well as the programs and transactions used to manipulate specific data. MSFR resource access control features allow users and administrators to specify, for each named resource, a list of individual users or groups of individual users that have access or have been explicitly denied access to that resource.
- In addition, a least privilege feature is specified that allows an association of privileges with named users that are limited and consistent with their functional job responsibilities.

2.4.3 Threats Countered by Accountability and Audit

- Accountability and audit requirements provide protection against the threat of an authorized user who, using his or her assigned privileges, performs some act that is detrimental to the organization. For instance, an officer of a bank may modify the balance of an accomplice's account, or an assistant within a medical office may divulge a patient's medical records without proper authorization. In either case, a system user is taking advantage of certain privileges that have been granted to him or her.

- MSFR accountability and audit features are specified to track security relevant actions performed by users and to link such actions to the responsible user. Audit features are specified to provide post-collection audit analysis on specific data items, users, and communications facilities. In addition, MSFR requirements specify real-time monitoring and reporting of events that may indicate a security violation requiring immediate administrative attention.

2.4.4 Threats Countered by Object Reuse

- Scavenging exists when a user searches a computer system for information that has been unintentionally made available. This can occur when residual information is left behind during the processing of sensitive information, by taking advantage of a system that is poorly managed, or when security features are not present to protect information properly.
- For example, scavenging can occur by gaining access to information in a computer system after the execution of a job. It can be accomplished by searching for residual data left by a process after its execution. This threat exploits an operating system that may not clear memory prior to reallocation into a user's memory space. Many computer systems do not clear disk or tape storage for performance reasons. In these cases, new data is written over old data. The threat is that programs can be designed or users may perform operations that will read old data from memory or storage prior to it being overwritten.
- Through the utilization of object reuse security features, this problem can be virtually eliminated. This security feature ensures that the memory contents are cleared of any residual data prior to introduction in a new user's address space.

2.4.5 Threats Countered by Accuracy

- Data and system integrity features are specified to provide protection against an unauthorized or undesired modification of system data. Such features include process isolation, audit and diagnostic facilities, system configuration checks and controls, as well as encryption and checksum facilities for use by application programs, administrators and end-users.

2.4.6 Threats Countered by Reliability of Service

- Reliability requirements are specified to promote the continued accessibility of system resources by authorized entities. These requirements principally counter threats related to intentional or unintentional denial of service attacks, but may also be useful against natural disasters. Requirements include: detection and reporting facilities, features to monitor and control the consumption of disk space and CPU usage, recovery mechanisms, and software and data backup and restoration facilities.

2.4.7 Threats Countered by Data Exchange

- Data exchange requirements are specified to promote the secure transmission of data over communication channels.
- Data encryption facilities provide a capability to protect against an unauthorized interception of information on a communication medium. The threat of wiretapping can be greatly mitigated through either physically protecting the communication line or use of encryption. Physical protection is often difficult to enforce because of the need to closely monitor all network components, including cables, which in the case of wide area networks is virtually impossible. It is also difficult to physically protect against improper monitoring of the network by nodes that are otherwise authorized to use the network. For this reason an encryption facility has been specified by the MSFR. In addition, system encryption facilities can be used for transmission of authentication data.
- The MSFR specifies requirements for error detection protocols to allow the capability to protect against an unauthorized or unexpected modification on a communication channel.
- The MSFR provide protection against the problem known as spoofing. This problem involves emulating an environment a user expects to see in order to capture the user's input. For instance, spoofing can occur when an innocent user is tricked into believing he or she is communicating with authorized operating system software, when in reality he or she is interacting with some malicious user's code. The intent of this code could be to capture logon data by printing a message like the operating system would normally print, requesting the user to logon or type the password.
- The MSFR specifies a direct communication channel between the user and the operating system to counter spoofing threats. This security feature ensures that a system user at a terminal is communicating directly with security relevant software instead of someone's malicious application program.

3. SPECIFICATION OF SECURITY ENFORCING FUNCTIONS

- This section follows the format of the ITSEC Security Target description in Sections 2.18 - 2.22, "Specification of Security Enforcing Functions." The ITSEC assumes that the specific functions described here have been selected to match the "Product Rationale" in the preceding Section 2. The Product Rationale is a discussion of the intended use of the product in an assumed environment with assumed threats. The specific set of Security Enforcing Functions then is selected to provide adequate security for such use. It is divided into eight generic headings, each covered in one of the following sub-sections. Each of the eight generic headings has a high level control objective followed by an extensive set of detailed security requirements. The developer may choose to comply with the high level control objective or the detailed requirements. Either approach or a combination of compliance with higher level control objectives in some sub-sections and detailed specific requirements

guidance in others is possible.

- By directing compliance towards the higher level control objectives in lieu of meeting detailed requirements, the product developer/vendor takes advantage of the fact that every problem can have a number of solutions. Some of these solutions are in the form of technological advances. This more general approach promotes innovation on the part of the developer and provides flexibility on the part of the evaluator. This approach may require the developer to provide substantial demonstration of compliance with the control objectives, including the possibility of extensive negotiation between the evaluator and the developer. Compliance with the control objectives clearly involves a greater risk for the vendor, as more is left to the judgment of the assessor.
- In contrast, the detailed requirements provide a more straightforward predetermined approach to compliance with security objectives. This approach provides a lower risk path for the developer by minimizing the negotiation process and potentially allowing for more rapid evaluation. Additionally, this approach promotes uniform evaluations over time and across multiple laboratories.

3.1 Identification and Authentication

The system shall establish and verify the claimed identity of a user. The user shall be required to provide a unique user ID, which the system shall use to identify the user. The user shall also be required to provide authentication information, e.g., a password, that is known by the system to verify the user's identity. The system shall protect identification and authentication information from unauthorized access or modification.

3.1.1 Identification

A user identification is a unique, auditable representation of the user's identity within the system. All system users, both individuals and remote machines, shall be uniquely identified to support individual accountability.

- 1. Unique user identification codes (userIDs) shall be utilized to identify individuals and remote machines. ®
- 2. The system shall require users, i.e., individuals and remote machines, to identify themselves with their assigned userID before performing any actions. ®
- 3. The system shall internally maintain the identity of all currently active users. ®
- a. Every process running on the system shall have associated with it the identity of the user under whose authorization the process is running, i.e., the invoking user or the userID associated with the invoking process. ®
- 4. The system shall disable userIDs after a period of time during which the userID has not been used. The time period shall be customer-specifiable with a default of 60 days. ®

- a. A complementary mechanism or procedure for the reinstatement or deletion of disabled userIDs shall also be provided. ®
- 5. The system shall provide a mechanism to temporarily disable userIDs. ®
- a. The mechanism that disables userIDs shall provide an option for automatic reactivation.®
- 6. A mechanism shall be available to provide the status, e.g., active, inactive, revoked, etc., of any valid userID. ®
- 7. The system shall support a mechanism that limits the number of multiple logon sessions for the same userID. The mechanism shall allow the System Administrator to specify separate limits for individual users and groups of users. The system-supplied default shall limit each user to one simultaneous logon session. ®
- 8. If the system provides a mechanism for dynamically changing userIDs, then it shall also provide a mechanism for limiting the users who may change to a userID that would provide privileged status. ®
- 9. A mechanism shall be available for the System Administrator to associate customer-defined identifying information, e.g., user name and affiliation, with each user identification code. ®
- 10. The system shall support a mechanism that allows userIDs to be grouped together into named groups. ®
- a. A userID shall be able to be associated with more than one group. ®
- b. A mechanism shall be available for the System Administrator to modify the group membership of a userID. ®
- c. A mechanism shall be available to list the names of all groups. ®
- d. A mechanism shall be available to list the membership of any group. ®

3.1.2 Authentication

- 1. The system shall provide a mechanism to authenticate the claimed identity of a user. ®
- 2. The system shall be able to incorporate and utilize alternate authentication mechanisms such as smart-card, biometrics, or trusted third-party techniques, i.e., the system shall have the ability to securely branch to non-vendor-supplied code during authentication. ®
- a. If multiple authentication mechanisms are available within the system, the System Administrator shall be able to specify the authentication mechanism to be used for specific users and groups. ®
- 3. The system shall protect all internal storage of authentication data so that it cannot be accessed by any unauthorized user. ®
- 4. The system shall support an application program interface to an authentication mechanism that uses passwords and meets the requirements outlined in section 3.1.2.1. ®

3.1.2.1 Password Requirements

- Systems are not required to use password mechanisms to authenticate user identities. Other authentication methods such as smart cards, cryptographic

based authentication, and biometrics provide stronger authentication and are becoming increasingly more common. However, password systems are the most often used authentication mechanism for system access. Password systems are also sometimes used for access control to sensitive data or transactions. If a password mechanism is used by the system, the following requirements are meant to provide for proper and secure utilization of that mechanism.

- 1. The system shall not provide a mechanism whereby a single stored password entry is explicitly shared by multiple userIDs. ®
- a. The system shall not, in any other way, facilitate the sharing of passwords by multiple users. ®
- 2. The system shall not prevent a user from choosing a password that is already associated with another userID. ®
- a. The system shall not provide any indication that a password is already associated with another userID. ®
- 3. The system shall store passwords in a one-way encrypted form. ®
- a. Encrypted passwords shall not be accessible to non-privileged users. ®
- b. Unencrypted passwords shall not be accessible to any users including the System Administrator. ®
- 4. The system shall automatically suppress or fully blot out the clear-text representation of the password on the data entry device. ®
- 5. The system, by default, shall not allow null passwords during normal operation. ®
- 6. The system shall provide a mechanism to allow passwords to be user-changeable. This mechanism shall require re-authentication of the user identity. ®
- a. The System Administrator shall have a mechanism to reset passwords for users. ®
- 7. The system shall enforce password aging on a per-user or per-group basis, i.e., a user's password shall be required to be changed after an administrator specifiable minimum time. The system-supplied default for all non-privileged users shall be 60 days. ®
- a. The system-supplied default for those userIDs that may acquire privileges shall be 30 days.®
- b. After the password aging threshold has been reached, the password will no longer be valid and system administrator action shall be required to reset the password. ®

- 8. The system shall provide a mechanism to notify users in advance of requiring them to change their passwords. ®
- This can be done by either:
- a. Notifying users a customer-specifiable period of time prior to their password expiring. The system-supplied default shall be 7 days. ®
- b. Upon password expiration, notifying the user but allowing a customer-specifiable subsequent number of additional usages prior to requiring a new password. The system-supplied default shall be 2 additional usages. ®
- 9. Passwords shall not be reusable by the same individual for a customer-specifiable period of time. The system-supplied default shall be six months. ®
- 10. The system shall provide a method of ensuring the complexity of user-entered passwords that meets the following requirements:
- a. Passwords shall meet a customer-specifiable minimum length requirement. The system-supplied default minimum length shall be eight characters. ®
- b. The password complexity-checking algorithm shall be modifiable by site. The system-supplied default shall require passwords to include at least one alphabetic character, one numeric character, and one punctuation character. ®
- c. The system should provide a mechanism to prevent user selection of customer-specified password exclusions, e.g., company acronyms, common surnames, etc. (A)

11. If system-supplied password generation algorithms are present in the system, they shall meet the following requirements: ®

a. The password generation algorithm shall generate passwords that are easy to remember, i.e., pronounceable or pass-phrases. ®

b. The system should give the user a choice of alternative passwords from which to choose. (A)

c. Passwords shall be reasonably resistant to brute-force password guessing attacks, i.e., the total number of system-generated passwords shall be on the same order of magnitude as what a user could generate using the rules specified in requirement 10 above. ®

d. If the "alphabet" used by the password generation algorithm consists of syllables rather than characters, the security of the password shall not depend on the secrecy of the alphabet. ®

e. The generated sequence of passwords shall have the property of randomness, i.e., consecutive instances shall be uncorrelated and the sequences shall not display periodicity. ®

3.2 Access Control

The system shall ensure that users and processes acting on their behalf are prevented from gaining access to information or resources for which they are not

authorized. The system shall be capable of controlling access to the granularity of a single user. Identification and authentication shall take place prior to other interactions between the system and the user.

Access to the system and other resources shall be limited to those users that have been authorized for that specific access right.

3.2.1 System Access Control

System access control is the process of determining which users have access to the system and when they have that access. It is usually during "system access" control execution that a user is solicited for their userID and password.

- 1. The identity of all system users shall be authenticated prior to their initially gaining access to the system. ®
- a. Remote machines shall be authenticated prior to establishment of an inter-system connection. ®
- 2. The system shall provide a mechanism to define users and remote machines that are authorized to access the system. ®.
- a. The system shall only allow access to those authorized users and authorized remote machines.®
- b. The system shall provide a mechanism that will list all users and remote machines that are authorized to access the system. ®
- 3. The system shall provide the capability to allow access to the system via specific customer-defined applications such that the applications' access control security policies take precedence over these requirements, i.e., section 3.2.1. ®
- 4. The system shall not provide any default userIDs that permit unauthenticated system access. ®
- 5. The system's logon procedure should be able to be reliably initiated by the user, i.e., a trusted communications path should exist between the system and the user during the logon procedure. (A)
- 6. The system shall disconnect or re-authenticate users after a customer-specifiable period of non-use. The system-supplied default shall be 15 minutes. ®
- 7. The system shall provide a mechanism for user initiated keyboard locking. ®
- a. The keyboard unlock procedure shall require user authentication. ®
- 8. The system logon procedure shall exit and end the session if the user authentication procedure is incorrectly performed a customer-specifiable number of times within a logon session. The system-supplied default shall be 3 times. ®
- a. The system shall provide a mechanism to immediately notify the System Administrator when this threshold is exceeded. ®
- b. When the above threshold has been exceeded, a customer-specifiable interval of time, not to exceed 60 seconds, shall elapse before the logon process can be restarted on that I/O port.®

- i. The system should provide a capability to increment the time interval on successive violations. (A)
- c. The system shall not suspend the userID upon exceeding the above threshold. ®
- 9. The system shall perform the entire user authentication procedure even if the userID that was entered was not valid. ®
- a. Error feedback shall not reveal which part of the authentication information is incorrect. ®
- 10. The system shall provide a mechanism to exclude or include users based on:
- a. time-of-day ®
- b. day-of-week ®
- c. calendar date ®
- 11. The system shall provide a mechanism to exclude or include users based on method or location of entry.®
- a. The system shall provide a mechanism to limit the users authorized to access the system via dial-up facilities. ®
- b. The system shall provide a mechanism to limit the users authorized to access the system via network facilities. ®
- 12. The system shall provide a mechanism to limit system entry for privileged users based on method or location of entry. ®
- a. The system-supplied default shall limit System Administrator userIDs to access from the system console only. ®
- 13. The system shall provide a mechanism to restrict specified users or groups of users to non-modifying access only. ®
- a. This mechanism shall be limited to the System Administrator. ®
- 14. If network access, e.g., dial-in, X.25, or INTERNET, is provided by the system, the system shall provide a stronger authentication mechanism that can be used at the customer's discretion. For example, the authentication mechanism can be a private or public key encryption-based mechanism, an additional password, dial-back, and/or smart card to validate the user or remote machine. ®
- a. The networking software shall be able to be disabled or configured out of the system. ®
- b. If network access is provided, a mechanism shall exist to end the session through secure logoff procedures. ®
- 15. The system shall provide an advisory warning message upon system entry regarding unauthorized use, and the possible consequences of failure to meet those requirements. ®
- a. The message shall be customer-specifiable to meet their own requirements and state laws. ®
- b. The system shall be able to display a message of up to twenty lines in length. This message shall be displayed at the first point of entry. If possible, the message shall appear before the logon process. As part of delivered software, the following default message shall be included: ®
- NOTICE: This is a private computer system. Unauthorized access or use may

lead to prosecution.

- 16. Upon successful access to the system:
- a. The date, time and location of the user's last successful system access shall be displayed. ®
- b. The number of unsuccessful attempts by that userID to access the system since the last successful system access by that userID shall be displayed. ®
- c. The number of days until the password expires shall be displayed. ®
- 17. A procedure shall be supplied for the initial entry or modification of authorized users and authentication information. ®
- 18. The system shall allow only the System Administrator or other well-defined privileged users, e.g., Application or Group Administrators, to authorize or revoke users. ®
- a. Procedures for adding and deleting users shall be well-defined and described in the System Administrator's security documentation. ®
- b. Only the System Administrator or other well-defined privileged users, e.g., Application Administrators, shall be able to modify user security profiles or change any other user security information. ®

3.2.2 Resource Access Control

Once a user has been identified and authenticated, the system shall mediate what data is visible to that user and what programs or transactions can be used by that user to manipulate data. The resource access control requirements are intended to address these concerns.

- 1. The system shall control access to all resources recognized by the system. ®
- 2. Control of access to resources shall be based on authenticated user identification. ®
- 3. For each resource controlled by the system, it shall be possible to specify a list of individual users or named groups of individual users with their specific access rights to that resource. ®
- a. The access rights that may be specified shall at a minimum include read, write, and execute. ®
- i. There should be separate create and delete access rights for modification of directories or catalogs. (A)
- ii. There should be a distinct access right required for a user, other than the owner of the resource, to modify the contents of the access control list. (A)
- iii. The system should support the explicit denial of all access rights to an individual user or named group. (A)
- b. The access rights associated with an individual user take precedence over the access rights associated with any groups of which that user is a member. ®
- c. For systems where a user can be a member of multiple groups simultaneously, if any named group entry allows an access right for that user, then the user is allowed that right (subject to "b" above). ®
- d. The system shall provide a mechanism to specify default access rights for

users not otherwise specified either explicitly by userID or implicitly by group membership. ®

- 4. Authorization of access to a resource shall occur at least upon "open" of the resource. ®
- 5. The system shall provide a mechanism that allows a user who creates a resource control of the access rights given to that resource. ®
- a. If no specific access rights are specified at resource creation, the default shall be that only the creator has access. ®
- 6. Explicit user action by the owner of the resource or by the appropriate privileged users, e.g., the System Administrator, Application Administrators, etc., shall be required to provide additional access rights to a resource. ®
- 7. Access to resources should be able to be controlled by:
- a. method or location of accessing user (A)
- b. time-of-day (A)
- c. day-of-week (A)
- d. calendar date (A)
- e. specific program used to access the resource (A)
- 8. The security attributes of a resource shall be preserved when a copy of that resource is made. ®
- 9. For each authorized user of the system, it shall be possible to identify all resources in the system that are either owned by that user or to which that user is granted explicit access rights. ®
- a. The associated access rights granted to that user shall also be provided. ®
- b. This mechanism shall be limited to the System Administrator. ®
- 10. The system shall provide a mechanism to remove access rights to all resources for a user or a group of users. ®
- a. This mechanism shall be limited to the System Administrator. ®
- 11. Access to any system-supplied resource shall be, by default, as limited as possible to permit the effective usage of the system and/or resource. ®
- 12. The access control mechanism's data files and tables shall be protected from unauthorized access. ®

3.2.3 Privileges

A privilege mechanism allows the system to assign a user only the privileges necessary to accomplish the task at hand and no more. Sets of privileges can be bundled together to define functional job responsibilities such as System Administrator, Security Administrator, Operator, etc.

- 1. The system shall support a privilege mechanism that meets the following requirements:
- a. Separate privileges shall be associated with groups of related security relevant operations or commands. ®
- i. Separate and distinct privileges should be associated with distinct security relevant operations. (A)
- ii. Privileges that permit overriding or bypassing the access control

mechanisms should be distinct and separate from any and all other privileges. (A)

- b. A user shall be assigned a privilege in order to invoke the corresponding operation. ®
- i. There should be a programmatic interface that allows the dynamic assignment of privileges to processes. (A)
- 2. The system shall support a mechanism that allows the System Administrator to associate privileges with named users. ®
- 3. The minimum set of privileges required for an Operator and a System Administrator shall be defined and documented by the vendor. ®
- 4. The security functions performed by the System Administrator shall be identified and documented. ®
- a. The security functions performed by the System Administrator should be separable from the non-security functions performed by the System Administrator. (A)

3.3 Accountability

The system shall ensure that relevant information about actions performed by users, or processes acting on their behalf, can be linked to the user in question and the user held accountable. The system shall maintain information sufficient for after-the-fact investigation of loss or impropriety and provide individual user accountability for all security relevant events. The system shall protect this information from unauthorized access or modification.

- 1. The system shall generate a security audit trail that contains information sufficient for after-the-fact investigation of loss or impropriety and for appropriate management response, including personnel actions and pursuit of legal remedies. ®
- 2. The system shall provide end-to-end user accountability for all security relevant events. ®
- a. The user identification information associated with any system request or activity shall be maintained and passed on to any other connected systems so that the initiating user can be traceable for the lifetime of the request or activity. ®
- 3. The audit trail shall be protected from unauthorized access.
- ®
  - a. Only the System Administrator shall be authorized to modify or delete the audit trail. ®
  - b. The system should support an option to maintain the audit trail data in encrypted format. (A)
- 4. The System Administrator shall be able to dynamically control during normal system operation the types of events recorded. This control shall include selective disabling of the recording of default audit events and the enabling and disabling of other optional events.®
- 5. The audit control mechanisms shall be protected from unauthorized access.

®

- 6. The system shall, by default, cause a record to be written to the security audit trail for at least each of the following events:
- a. Invalid user authentication attempts ®
- b. Logons and activities of privileged users, e.g., System Administrators, Operators ®
- c. Unsuccessful data or transaction access attempts ®
- d. Successful accesses of security-critical system resources ®
- e. Changes to users' security profiles, privileges, or attributes ®
- f. Changes to access rights of resources ®
- g. Changes to the system security configuration ®
- h. Modification of system-supplied software ®
- 7. The System Administrator shall have the capability to enable or disable the recording of other optional events into the audit trail which include at a minimum:
- a. Valid user authentication attempts ®
- b. Creation and deletion of resources ®
- c. Disk file access ®
- d. Tape volume or tape file access ®
- e. Program execution ®
- f. On-line command execution ®
- g. Customer-defined events ®
- 8. For each recorded event, the audit record shall identify, at a minimum:
- a. Date and time of the event ®
- b. User identification and associated point of physical access, e.g., terminal, port, network address, or communication device ®
- c. Type of event ®
- d. Name of resources accessed ®
- e. Success or failure of the event ®
- 9. It shall not be possible to disable the auditing of Administrator actions. ®
- a. Any modification to the set of auditable events shall always be audited. ®
- 10. Actual or attempted passwords shall not be recorded in audit trails. ®
- 11. Audit control data, e.g., audit event masks, shall survive system restarts. ®
- 12. The system shall provide a mechanism for automatic copying of audit trail files to an alternate storage medium after a customer-specifiable period of time.®
- a. The system shall provide a mechanism for automatic deletion of audit trail files after a customer-specifiable period of time. The system-supplied default shall be 30 days. ®
- 13. The system shall allow site control of the procedure to be invoked when audit records are unable to be recorded. ®
- a. The system shall generate an alarm to the System Administrator if audit records are unable to be recorded. ®
- 14. The system shall provide tools for the System Administrator to monitor the activities of specific terminals or network addresses in real time. ®

3.4 Audit

The system shall provide a mechanism to determine if security violations have actually occurred, and if so, what information or other resources were compromised.

- 1. The system shall provide post-collection audit analysis tools that can produce exception reports, summary reports, and detailed reports on specific data items, users, or communications facilities. ®
- 2. The System Administrator shall be able to independently and selectively review the actions of any one or more users, including privileged users, based on individual user identity. ®
- 3. The system shall be able to provide a report of all modifications to any named or user-accessible system resources. ®
- 4. The system should contain a real-time mechanism that is able to monitor the occurrence or accumulation of security relevant events that may indicate an imminent security violation. This mechanism should be able to immediately notify the System Administrator when thresholds are exceeded, and, if the occurrence or accumulation of these security relevant events continues, the system should take the least disruptive action to terminate the event. (A)

3.5 Object Reuse

The system shall ensure that resources can be reused while preserving security. Resources that are allocated to a user shall not contain any information related with prior usage by the system or another system user.

- 1. The system shall ensure that non-privileged users are not able to reference the contents of a resource that has been returned to the system after usage. ®
- 2. The system shall ensure that non-privileged users are not able to reference the prior contents of a resource that has been allocated to that user by the system. ®

3.6 Accuracy

The system shall protect against unauthorized or undesired modification of data. This includes protection against all modifications of the system itself and the data maintained by the system that are not the intent of the systems authorized users.

- 1. The system shall provide mechanisms to separate and protect a given user's programs and data from other users' programs. ®
- a. The system shall provide mechanisms to separate and protect the system's programs and data from any user's programs. ®
- 2. Procedures, e.g., use of modification dates, permissions, checksums, etc., shall exist that make it possible to verify that the currently installed software has remained consistent with the delivered software, i.e., no unauthorized

modifications have been made. ®

- 3. The system shall restrict usage of:
- a. Privileged instructions ®
- b. Supervisory state ®
- c. I/O instructions ®
- 4. The system shall control and audit usage of the system operator's console. ®
- 5. The ability to execute system-supplied utilities shall be, by default, as limited as possible to permit the effective usage of the system. ®
- a. The ability to modify or replace system-supplied utilities shall be limited to only the System Administrator. ®
- 6. The system shall provide the capability to restrict or control the modification or replacement of the operating system software including any firmware. ®
- 7. The system shall provide a mechanism for users to control the order of directory/path search for command resolution. ®
- a. The System Administrator shall be able to disable user-control of this mechanism on a per-user basis. ®
- 8. The system shall be able to provide the date and time of the last modification to any named or user-accessible system resource. ®
- a. The system should be able to provide the userID of the user that made the last modification to any named or user-accessible system resource. (A)
- 9. A checksum mechanism shall be available to application programs and users. ®
- 10. Data encryption facilities that allow data to be stored in an encrypted format shall be available to application programs and users. ®
- 11. The system shall provide mechanisms or procedures that can be used to periodically validate the correct operation of the system. ® These mechanisms or procedures shall address:
- a. Monitoring of system resources ®
- b. Correct operation of on-site hardware and firmware elements ®
- c. Detection of error conditions that might propagate throughout the system ®
- d. Detection of communication errors above a customer-specifiable threshold ®
- 12. The system shall provide a utility for checking file system and disk integrity, e.g. FSCK. ®
- a. This utility shall be run automatically by vendor-supplied software. ®
- 13. The system shall provide a mechanism for the System Administrator to generate a status report detailing the values of all configurable security parameters. ®

3.7 Reliability of Service

The system shall promote the continuous accessibility and usability of resources on demand by an authorized entity, i.e., a user or a process acting on his/her behalf, and shall prevent or limit interference with time-critical operations.

The system shall maintain its expected level of service in the face of any user action either deliberate or accidental.

- 1. No non-privileged user-level action, either deliberate or accidental, shall cause the system to be unavailable to other users other than as specified by the requirements. ®
- 2. The system should detect and report conditions that degrade service below a System Administrator specifiable minimum.
  - (A)
- 3. The system shall provide a mechanism for controlling consumption of disk space and CPU usage on a per-user and per-group basis. ®
- 4. Procedures or mechanisms shall be provided to allow recovery after a system failure or other discontinuity without a security compromise. ®
- 5. The system shall provide the capability of running in an administrative maintenance mode with all security features disabled. ®
- a. The system shall be accessible only to System Administrators during administrative maintenance mode. ®
- 6. Procedures shall be provided for software and data backup and restoration. ®
- 7. Synchronization points, e.g., checkpoint restarts, shall be added to software systems to facilitate recovery. ®

3.8 Data Exchange

The system shall promote the secure transmission of data over communications channels.

- 1. The system shall be able to identify the originator of any information received across communications channels. ®
- 2. Data encryption facilities shall be available that allow data to be sent across communications channels in an encrypted format. ®
- 3. All authentication data shall be communicated directly from the point-of-entry to the authenticating system. ®
- a. Authorization data sent over public or shared data networks shall be encrypted. ®
- 4. Error detection protocols shall be available when sending information across communications channels. ®
- 4. OTHER SECURITY TARGET REQUIREMENTS
- In order for the MSFR Security Target to be consistent with ITSEC requirements, the following additional information is provided.
  - 4.1 Required Security Mechanisms
- There are no required security mechanisms in the MSFR Security Target. Prescription of such specific mechanisms is optional in Security Targets, and is not used here.
- 4.2 Minimum Strength of Mechanisms
- The claimed rating for minimum strength of security mechanisms that product

Targets of Evaluation (TOE) which use this Security Target are expected to meet is basic, as described in Section 3.6 of the ITSEC. Such TOEs should provide protection against random accidental subversion, but may be capable of being defeated by knowledgeable attackers.

- 4.3 Target Level of Evaluation-
- Minimum Security Assurance Requirements
- The TCSEC and ITSEC recognize that the presence of desired security features alone are not sufficient for establishing the potential value of a computer product for protecting information. Underlying the security features must be a process of product development and assessment to provide assurance that the security features actually work as claimed and that no other security flaws were included as a result of the development process. The requirements that constrain the product development and assessment processes and specify the evidence to be produced as a result of the processes are commonly called assurance requirements.
- A Minimum Security Assurance Requirements (MSAR) section will be included in the FC-FIPS for use with the MSFR, in lieu of the ITSEC requirement to specify a Target Evaluation Level from E1 to E6. The MSAR is currently under development by the MSR Working Group and is not ready for public review. It is currently envisioned that these minimum assurance requirements will be based on a convergence of TCSEC C2 requirements and the ITSEC E2 level, with special emphasis on lifecycle needs. These assurance requirements will be included in the draft FC-FIPS circulated for public comment.

5. GLOSSARY

- Access control. The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. [ISO] Access control mechanisms are used to allow, deny, or limit individuals and remote machines access to a resource. Access control mechanisms are typically based on the authenticated identity of the individual or remote machine requesting access. In this document, the terms access control and authorization are synonymous.
- Access control list. A list of entities, together with their access rights, which are authorized to have access to a resource. [ISO]
- Accountability. The property that ensures that the actions of an entity may be traced uniquely to the entity. [ISO] Administration Documentation. The information about a system supplied by the vendor for use by a system administrator. [ITSEC]
- Application Program Interface. A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality. Architectural Design. A phase of the Development Process wherein the top level definition and design of a system is specified. [ITSEC]
- Assurance. The confidence that may be held in the security provided by the system. [ITSEC]

- Audit. See security audit.
- Audit trail. See security audit trail.
- Authentication. Authentication is the process of proving the claimed identity of an individual user, machine, software component or any other entity. Typical authentication mechanisms include conventional password schemes, biometrics devices, cryptographic methods, and onetime passwords (usually implemented with smart cards.)
- Authentication information. Information used to establish the validity of a claimed identity. [ISO]
- Authorized. Entitled to a specific mode of access.
- Authorization. The granting of rights. [ISO] Authorization mechanisms are used to allow, deny, or limit individuals and remote machines access to a resource. Authorization mechanisms are typically based on the authenticated identity of the individual or remote machine requesting access. In this document, the terms access control and authorization are synonymous.
- Availability. The property of being accessible and usable upondemand by an authorized entity. [ISO] The prevention of theunauthorized withholding of information or resources. [ITSEC]Channel. An information transfer path within a system. May alsorefer to the mechanism by which the path is effected. [TCSEC]Clear-text. Intelligible data, the semantic content of which isavailable. [ISO]
- Configuration. The selection of one of the sets of possiblecombinations of features of a system. [ITSEC]Configuration control. A system of controls imposed on changingcontrolled objects produced during the development, production,and maintenance processes for a system. [ITSEC]
- Cryptography. The discipline which embodies principles, means,and methods for the transformation of data in order to hide itsinformation content, prevent its undetected modification and/orprevent its unauthorized use. [ISO]
- Customer. The person or organization that purchases the system. [ITSEC]
- Data integrity. The property that data has not been altered or destroyed in an unauthorized manner. [ISO] Delivery. The process whereby a copy of the system is transferred from the vendor to the customer. [ITSEC] Denial of service. The prevention of authorized access to resources or the delaying of time-critical operations. [ISO]
- Detailed design. A phase of the Development Process wherein the top level definition and design of a system is refined and expanded to a level of detail that can be used as a basis for implementation. [ITSEC]
- Developer. The person or organization that manufacturers a system. [ITSEC]
- Development environment. The organizational measures, procedures, and standards used while constructing a system. [ITSEC]
- Development Process. The set of phases and tasks whereby a system is constructed, translating requirements into actual hardware and software. [ITSEC]
- Documentation. The written (or otherwise recorded) information about a system. The information may, but need not, be contained within a single document.

- Encryption key. See password.
- End-to-end user accountability. The property that ensures that the actions of an entity from initial system logon to system logoff may be traced uniquely to the entity even when those actions take place across a distributed system or network.
- End-user. A person in contact with a system who makes use only
- of its operational capability. [ITSEC]
- Functional testing. The portion of security testing in which the advertised features of a system are tested for correct operation. [TCSEC]
- Identification. The identification of an individual user, machine, software component or any other entity is a unique, auditable representation of identity within the system usually in the form of a simple character string.
- Implementation. A phase of the Development Process wherein the detailed specification of a system is translated into actual hardware and software. [ITSEC]
- Least privilege. A principle which requires that each user in a system be granted the most restrictive set of privileges and authorizations needed for the performance of authorized tasks.
- The application of this privilege limits the damage that can result from accident, error, or unauthorized use. [TCSEC]
- Operation. The process of using a system. [ITSEC]
- Operational Documentation. The information produced by the vendor of a system to specify and explain to customers how to use it. [ITSEC]
- Operating System. The term Operating System refers to the vendor developed and maintained control program of a computer system and its associated security support software. Where possible this document uses the term system to refer to the Operating System.
- Operational Environment. The organizational measures, procedures, and standards to be used while operating a system. [ITSEC]
- Password. Confidential authentication information, usually composed of a string of characters. [ISO]
- Password key. See password.
- Privileged User. User that is allowed additional data, transaction, or service access.
- Production. The process whereby copies of a system are generated for distribution to customers. [ITSEC]
- Programming Languages and Compilers. The tools used within the Development Environment in the construction of the software and/or firmware of a system. [ITSEC]
- Requirements. A phase of the Development Process wherein the top level definition of the functionality of the system is produced.
- Resource. A resource is any nameable entity under the control of the Operating System that can be accessed directly. Examples are: data sets, files, disks, tape drives, printers, floppy diskettes, programs, pipes, or memory.
- Security audit. An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance

with established policy and operational procedures, and to recommend any indicated changes in control, policy, and procedures. [ISO]

- Security audit trail. Data collected and potentially used to facilitate a security audit. [ISO] A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions. [TCSEC]
- Shall. The word shall indicates a requirement that shall be met unless a justification of why it cannot be met is given and accepted.
- Should. The word should indicates an objective more than a requirement. It is often used when a specific requirement is not feasible in some situations or with common current technology. Non-conformance to such requirements requires less justification and should be more readily approved.
- System Administrator. A person who is in contact with the system who is responsible for maintaining its operational capacity. [ITSEC]
- Threat. A potential violation of security. [ISO] An action or event that might prejudice security. [ITSEC]
- User Documentation. The information about a system supplied by the vendor for use by its end-users. [ITSEC]
- Vulnerability. A security weakness in a system (for example, due to failures in analysis, design, implementation, or operation). [ITSEC]

6. REFERENCES

[l] US Department of Defense Trusted Computer System Evaluation

Criteria (TCSEC), DoD 5200.28-STD, December 1985.

[2] Information Technology Security Evaluation Criteria

(ITSEC) - Provisional Harmonised Criteria, Version 1.2, June

1991.

[3] Assessing Federal and Commercial Information Security Needs,

Ferraiolo, D. and Gilbert, D., NIST Internal Report Draft,

December 6, 1991.

[4] Security Controls for Computer Systems: Report of Defense

Science Board Task Force on Computer Security, Willis Ware,

Editor, R-609-1, 1970, Reissued October 1979.

[5] Computers at Risk - Safe Computing in the Information Age, National Research Council, National Academy Press, 1991.

[6] Commercial International Security Requirements (CISR), Cutler, K. and Jones, F., Final Draft, September 9, 1991.

[7] Bellcore Standard Operating Environment Security Requirements, TA-STS-001080, Issue 2, June, 1991.

[8] Information Processing Systems - Open Systems Interconnection Reference Model - Part 2: Security Architecture, International Standard 150 7498-2, International Organization for Standardization, 1988