National Nuclear Security Administration

NNSA Policy Letter: NAP-14.6
Date: September 12, 2003

TITLE: Unclassified Mandatory Protection Information Group Protection Profile

1. OBJECTIVE. Establish requirements for the protection of National Nuclear Security (NNSA) Unclassified Mandatory Protection information when information systems are used to collect, create, process, transmit, store, and disseminate this information.

2. APPLICABILITY. This NNSA Policy (NAP) applies to all entities, Federal or contractor, which collect, create, process, transmit, store, and disseminate NNSA information.

   a. NNSA Elements. NNSA Headquarters Organizations, Service Center, Site Offices, NNSA contractors, and subcontractors are, hereafter, referred to as NNSA elements.

   b. Information System. This NAP applies to any information system that collects, creates, processes, transmits, stores, and disseminates unclassified or classified information for NNSA. This NAP applies to any information system life cycle, including the development of new information systems, the incorporation of information systems into an infrastructure, the incorporation of information systems outside the infrastructure, the development of prototype information systems, the reconfiguration or upgrade of existing systems, and legacy systems. In this document, the term(s) "information system," or "system" are used to mean any information system or network that is used to collect, create, process, transmit, store, or disseminate data owned by, for, or on behalf of NNSA or DOE.

   c. Deviations. Deviations from the requirements prescribed in this NAP must be processed in accordance with the requirements in Chapter VIII, NAP-14.1, *NNSA Cyber Security Program.*

   d. Exclusion. The Deputy Administrator for Naval Reactors shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (set forth in Public Law 106-65 of October 5, 1999 [50 U.S.C. 2406]) and to ensure consistency throughout the joint Navy and DOE Organization of the Naval Reactors Propulsion Program, implement and oversee all requirements and practices pertaining to this policy for activities under the Deputy Administrator's cognizance.

   e. Implementation. A plan for the implementation of this NAP must be completed within 60 days after issuance of this NAP.

3. RESPONSIBILITIES. Roles and responsibilities for all activities in the NNSA PCSP are described in NAP-14.1, *NNSA Cyber Security Program.*

4. REQUIREMENTS. The attached Protection Profile (PP) defines the requirements for protecting NNSA information in the Unclassified Mandatory Protection Information Group and the information systems used to collect, create, process, transmit, store, and disseminate this information.

5. CONTACT. Questions concerning this NAP should be directed to the NNSA Cyber Security Program Manager at 202-586-4775.

Linton Brooks
Administrator

Attachments

National Nuclear Security Administration

PROTECTION PROFILE

FOR THE

UNCLASSIFIED MANDATORY PROTECTION INFORMATION GROUP

National Nuclear Security Administration

Version	Revision Date	Description/ Change
1.0	03/31/03	Version 1.0 – Initial Release

Foreword

This publication, "Protection Profile for Unclassified Mandatory Protection Information," is issued by the Department of Energy/National Nuclear Security Administration as part its Program Secretarial Office Cyber Security Program to promulgate protection standards for information.

The base set of requirements used in this protection profile is taken from the "Common Criteria for Information Technology Security Evaluations, Version 2.0." Further information about the Common Criteria can be found on the Internet at http://csrc.nist.gov/cc/index.html.

Table of Contents

1. PP Introduction

This Unclassified Mandatory Protection Information Group[1] Protection Profile, hereafter called MANDPP, specifies a set of security functional and assurance requirements for the NNSA Unclassified Mandatory Protected Information Group and the Information Technology (IT) products used to create, store, process, disseminate information in this Information Group.

This section contains document management and overview information necessary to describe the Protection Profile (PP) for use in the National Nuclear Security Administration (NNSA). The PP identification provides the labeling and descriptive information necessary to identify, catalogue, register, and cross-reference a PP. The PP overview summarizes the profile in narrative form and provides sufficient information for a potential user to determine whether the PP is of interest. The overview can also be used as a standalone abstract for PP catalogues and registers. The conventions section provides an explanation of how this document is organized and the terms section gives a basic definition of terms that are specific to this PP.

1.1 PP Identification

Title: NNSA Protection Profile for Unclassified Mandatory Protection Information (MANDPP)

Keywords: access control, discretionary access control, general-purpose operating system, information protection

1.2 PP Overview

Environments, systems and products conforming to the MANDPP support access controls that are capable of enforcing access limitations on individual users and data objects. MANDPP compliant systems also provide an audit capability that records the security-relevant events that occur within the system.

The MANDPP provides for a level of protection that is appropriate for an assumed non-hostile and well-managed user community requiring protection against threats of inadvertent or casual attempts to breach the system security. The profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well-funded attackers to breach system security. The MANDPP does not fully address the threats posed by malicious system development or administrative personnel. These threats must be mitigated by other technical and non-technical measures.

The MANDPP is generally applicable to distributed systems but does not address the security requirements that arise specifically out of the need to distribute the resources within a network.

---

[1] **Unclassified Mandatory Protection** -- Unclassified information requiring protection mandated by policy, laws, such as Privacy Act information; Agreements between Department of Energy (DOE), NNSA, its contractors, and other entities such as commercial organizations or foreign governments; Proprietary information (but not third party proprietary); Unclassified Controlled Nuclear Information (UCNI); Export-controlled information (ECI); Naval Nuclear Propulsion Information (NNPI); Military/ dual use information (such as the Critical Military Technology and Materials list identified by DoD); Nonproliferation information; and Information exempt from the Freedom of Information Act (FOIA),

1.3 Strength of Environment

The strength of environment is based on the NNSA Consequences of Loss minimums defined in the NNSA PCPS and the threats from the NNSA Cyber Risk Assessment. The assurance requirements and the minimum strength of function were chosen to be consistent with that level of risk.

The assurance level for MANDPP is NNSA AL 2 and the minimum strength of function is SOF-medium.

1.4 Conventions

This document is organized based on Annex B of Part 1 of the Common Criteria. For each component, an application note may appear. Application notes document guidance for how the requirement is expected to be applied. For additional guidance, the CC itself should be consulted.

1.5 Terms

This profile uses the following terms that are described in this section to aid in the application of the requirements:

- User
- Authenticated User
- Administrator
- Discretionary Access Control (DAC) Policy
- Access
- Authorization
- Category

A user is an individual who attempts to invoke a service offered by the TOE. An authenticated user is a user who has been properly identified and authenticated. These users are considered to be legitimate users of the TOE.

An administrator is an authenticated user who has been granted the authority to manage the TOE. These users are expected to use this authority only in the manner prescribed by the guidance given them.

2. TOE DESCRIPTION

The MANDPP defines a set of security requirements to be levied on Targets of Evaluation (TOEs) containing the Unclassified Mandatory Protection Information Group. These TOEs include information systems that are personal electronic devices, portable computers, and systems containing general-purpose operating systems, such as workstations, mainframes, or personal computers. These systems can be comprised of a single host or a set of cooperating hosts in a distributed system. Such systems permit one or more processors along with peripherals and storage devices to be used by single or multiple users to perform a variety of functions requiring access to the information stored on the system.

The MANDPP is applicable to TOEs that provide facilities for on-line interaction with users, as well as TOEs that provide for batch processing. The protection profile is also generally applicable to TOEs incorporating network functions but contains no network specific requirements. Networking is covered only to the extent to which the TOE can be considered to be part of a centrally managed system that meets a common set of security requirements.

The MANDPP assumes that responsibility for the safeguarding of the data protected by the TOEs security functions (TSF) can be delegated to the TOE users. All data is under the control of the TOE. The data are stored in objects, and the TSF can associate a description of access rights with each controlled object.

All individual users are assigned a unique identifier. This identifier supports individual accountability. Activities of all users of the TOE are subject to monitoring.

The TSF authenticates the claimed identity of the user before allowing the user to perform any actions that require TSF mediation, other than actions that aid an authenticated user in gaining access to the TOE.

3. TOE Security Environment

3.1 Assumptions

This section describes the security aspects of the environment in which the TOE will be, or is intended to be used. This includes information about the physical, personnel, and connectivity aspects of the environment.

A MANDPP-conformant TOE is assured to provide effective security measures in a cooperative non-hostile environment only if it is installed, managed, and used correctly. The operational environment must be managed in accordance with assurance requirements documentation for delivery, operation, and user/administrator guidance. The following specific conditions are assumed to exist in an environment where MANDPP-conformant TOEs are employed.

3.1.1 Physical Assumptions

MANDPP-conformant TOEs are intended for application in user areas that have physical control and monitoring. It is assumed that the following physical conditions will exist:

A.LOCATE	The processing resources of the TOE will be located within controlled access facilities that will prevent unauthorized physical access.
A.PROTECT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

3.1.2 Personnel Assumptions

It is assumed that the following personnel conditions will exist:

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.TRAINED_ADM	The system administrative personnel will follow and abide by the instructions provided by the administrator documentation.
A.COOP	Users possess the necessary authorization to access at least some of the information managed by the TOE and most users are expected in a benign manner.

3.1.3 Connectivity Assumptions

The MANDPP contains no explicit network or distributed system requirements. However, it is assumed that the following connectivity conditions exist:

A.PEER	Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints or that the TOE is isolated by appropriate barriers, such as controlled interfaces, firewalls, etc. MANDPP-conformant TOEs are applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements that address connectivity to external systems or the communications links to such systems. A Controlled Interface may be necessary to preserve this assumption.
A.CONNECT	All connections to peripheral devices reside within the controlled access facilities. MANDPP-conformant TOEs only address security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.

3.2 Threats

These threats are addressed MANDPP compliant TOEs. The threat agents are either human users or external IT entities not authorized to use the TOE itself. The asset that is subject to attack is the information residing on the TOE itself.

3.2.1 TOE Threats

T.ABUSE_ADMIN	System administrator abuse of privileges
T.ABUSE_OTHER	Compromise by authorized activities
T.ABUSE_USER	Abuse of authorized user privileges
T.ACCESS_MALICIOUS	Unauthorized access by an authenticated user for malicious purposes
T.ACCESS_NON_TECHNICAL	Unauthorized access by authenticated user through non-technical means
T.ACCESS_TOE	Unauthorized access by authorized user
T.ACCESS_UNDETECTED	Undetected perpetrator access
T.ATTACK_OTHER	Unauthorized action by perpetrator

T.AUDIT_CONFIDENTIALITY_TOE	Loss of audit trail confidentiality
T.AUDIT_CORRUPTED_TOE	Corruption of audit trail
T.AUTHENTICATION_NETWORK	Unauthenticated communications between client and server
T.CAPTURE	Eavesdropping
T.CONFIGURATION_ADMIN	Inadequate configuration management
T.CONSUME_OTHER	Resource access denial by excessive use
T.COVERT_OTHER	Covert channel use
T.CRASH	System crash
T.DELETE_UNINTENTIONAL	Unintentional user deletion or destruction
T.DENY_OTHER	Denial of participation in information transfer
T.DESIGN_LIMIT	Attack over and above system design limits
T.EAVESDROPPING	Unauthorized monitoring of networks or information systems
T.ENTRY_NON_TECHNICAL	Unauthenticated user gains access through non-technical means
T.ENTRY_OTHER	Inappropriate access by authorized user
T.ENTRY_SOPHISTICATED	Unauthenticated user gains access to other assets
T.ENTRY_TOE	Attack by unauthorized malicious user
T.ERROR_USER	User errors
T.EXPORT	Improper export of data
T.FLAWED_CODE	Flawed or incorrectly implemented software
T.IMPERSON_OTHER	Impersonation of authorized user
T.INSTALL	Insecure delivery or installation
T.INTEGRITY_OTHER	Compromise of data integrity
T.INTENTIONAL_DISCLOSURE	Intentional disclosure of data or software
T.LINK_OTHER	Analysis of observed activity
T.MAINTENANCE	Poor Maintenance
T.MALICIOUS_CODE	Malicious code

T.MASQUERADE_AUTHORIZED_USER	Masquerade of authorized user
T.MODIFY_OTHER	Unauthorized modification or destruction of data
T.NON_REPUDIATION_RECEIVE	Repudiation by authorized receiver
T.NON_REPUDIATION_SEND	Repudiation by authorized sender
T.NON_REPUDIATION_TRANSACTION	Repudiation of authorized transaction
T.OBSERVE_OTHER	Unauthorized observation of legitimate activities
T.OBSERVE_TOE	Misplaced/incorrect belief in secure operation
T.OPERATE	Improper operation of system
T.PHYSICAL	Unauthorized hardware change
T.PHYSICAL_ATTACK	Physical attack on system components and data
T.POWER_OTHER	Loss of power
T.RECORD_EVENT_TOE	Failure to record security significant events
T.RESOURCES_TOE	Exhaustion of system resources
T.SECRET_OTHER	Exposure of data to authorized user without need-to-know
T.SOCIAL_ENGINEERING	Social engineering attacks
T.SPOOFING	Spoofing of user identities, system components, and data
T.SPRINGBOARD	Use of information system to mount attacks on other systems
T.STEGANOGRAPHY	Steganographic exfiltration
T.SYSTEM_CORRUPTED	Intentional corruption of the system security state to enable future insecurities
T.TAMPER	Tampering with protection relevant system components
T.TOE_CORRUPTED	Corruption of system security status
T.TRACEABLE_TOE	Unable to trace events to users or processes
T.TRAPDOOR_BENIGN_ADMIN	Benign trapdoor installed by system administrator

T.TRAPDOOR_MALICIOUS_CODE

Malicious trapdoor provided by developer

T.UNAUTHORIZED_MALICIOUS_SOFTWARE

Unauthorized malicious software installed by user

T.UNINTENTIONAL_DISCLOSURE

Unintentional disclosure of data or software

T.UNINTENTIONAL_MALICIOUS_SOFTWARE

Unintentional malicious software installed by user

3.2.2 Non-TOE Threats

T.ACCESS_NON_TOE	Unauthorized access by authenticated user through other assets
T.AUDIT_CONFIDENTIALITY_NON_TOE	Unauthorized disclosure of non-TOE audit trails
T.CONFIGURATION_ADMIN	Inadequate configuration management
T.CRASH	System crash
T.DENIAL_NON_TOE	Denial of service against security support structure
T.ENTRY_NON_TECHNICAL	Unauthenticated user gains access through non-technical means
T.ENTRY_NON_TOE	Unauthenticated user gains unauthorized access to other assets
T.ENTRY_SOPHISTICATED	Unauthenticated user gains access to other assets
T.INSTALL	Insecure delivery or installation
T.LINK_OTHER	Analysis of observed activity
T.LOSS_SOFTWARE	Unintentional loss of software or application
T.MAINTENANCE	Poor Maintenance
T.MASQUERADE_AUTHORIZED_USER	Masquerade of authorized user
T.MODIFY_OTHER	Unauthorized modification or destruction of data

T.OBSERVE_NON_TOE	Misplaced/incorrect belief in secure operation of the security support structure
T.OBSERVE_OTHER	Unauthorized observation of legitimate activities
T.OPERATE	Improper operation of system
T.PHYSICAL	Unauthorized hardware change
T.PHYSICAL_ATTACK	Physical attack on system components and data
T.POWER_OTHER	Loss of power
T.RECORD_EVENT_NON_TOE	Failure to record security significant events on other assets
T.SECRET_OTHER	Exposure of data to authorized user without need-to-know
T.SOCIAL_ENGINEERING	Social engineering attacks
T.SPOOFING	Spoofing of user identities, system components, and data
T.SPRINGBOARD	Use of information system to mount attacks on other systems
T.TAMPER	Tampering with protection relevant system components
T.UNINTENTIONAL_DISCLOSURE	Unintentional disclosure of data or software

3.3 Organizational Security Policies

P.ACCOUNTABILITY	Users are held accountable for their actions, and actions taken on their behalf, on the information system.
P.ALT_INFRASTRUCT	Information system users have, based on mission need, continuing access to the information system hardware and software assets.
P.AUTH_MGMT	The process of generating, issuing, and using authenticators is managed in accordance with NNSA and site policies.
P.AUTHENTICATION	All users shall be authenticated prior to being granted access to systems and the information and resources managed by those systems.
P.COMPOSITION	The security of an information system or network composed of individual information systems is equal to or greater than that of any individual system in the combined system.
P.CONFIG_MGMT	Protection features of a system are maintained during development, modification, and maintenance of the hardware, firmware, and software components.

P.CONOPS	Continuity of operations planning is applied to applications, data, and information systems.
P.CREDENTIAL_PROTECTION	Authentication credentials shall be protected to prevent unauthorized access, modification or destruction. This policy requires that the individuals and IT entities that use the credentials adequately protect all credentials. The information system supports this policy by restricting access to credentials, by protecting the credentials as they are transmitted over the network during the domain authentication process, and through the trusted path between the credential reader and other information system components.
P.CRYPTOGRAPHY	Cryptographic services that are used to ensure information confidentiality, privacy or integrity shall meet the criteria of the appropriate robustness (strength of mechanism and assurance) based on the value of information to be protected and the threat environment.
P.CTL_INTERFACE	Protection requirements and adjudication of security policy differences are enforced when two or more information systems or networks are interconnected.
P.DATA_ASSURANCE	Modification of data is permitted only by authorized personnel.
P.DATA_AVAILABILITY	User and information system data are available, or restorable, to meet mission availability requirements
P.DENY_ACCESS	System resources are controlled to ensure access to information sources cannot be denied to authorized users.
P.DUE_CARE	The information and information system resources are implemented and operated in a manner that represents due care and diligence with respect to risks to the information and the organization.
P.FILE_REVIEW	An automated or administrative classification and sensitivity review is performed on all electronic communications and files that are to be electronically transmitted beyond the system boundary before release.
P.FORENSICS	Information needed for penetration reconstruction, and analyzing on-going or past cyber attacks and failures is identified, collected, and preserved in accordance with NNSA and site policies.
P.IDS	The information system is protected from unauthorized attempts to attack or penetrate the information system.
P.INFO_FLOW	Information flow between information system components is controlled in accordance with established information flow policies.

P.KNOWN	All NNSA multi-user information systems, desktops, and laptops– excluding those information systems intended to provide public access (e. g., public web servers)– must have, and use, a mechanism that authenticates the identity of each person before providing access to any information system, application, service or resource.
P.LEAST_PRIV	Privileges granted to information system users (including privileged users) are the most restrictive (least privilege) set of privileges needed for the performance of authorized tasks.
P.MALICIOUS_CODE	The information system is protected from hardware, software, and firmware designed to adversely impact the confidentiality, integrity, and availability of the system and information assets.
P.MEDIA_MARKING	All removable media components of the information system and output inside the system boundary are appropriately marked with the level of the highest information sensitivity of information that the system is accredited to operate; or marked in accordance with a classification review or information sensitivity review by authorized personnel.
P.MEDIA_REVIEW	All media (paper, disks, zip drives, removable disk drives, etc.) are reviewed for classification and sensitivity and properly marked before release outside the system boundary.
P.MONITORING	All users' activities, and activities on behalf of the user, are monitored and reviewed for activities that are detrimental to the confidentiality, integrity or availability of the information or information system.
P.NTK	Access to data in information system resources is limited to users with the need-to-know for the information, regardless of the form of the information. Access rights to specific data objects are determined by object attributes assigned to that object, user identity, user attributes, and environmental conditions as defined by the security policy.
P.PERSONNEL	All users (including privileged users) are cleared, or have appropriate background reviews, according to NNSA and DOE policies, for the highest level of information sensitivity, have formal access approval for, and an authorized need-to-know for, the information to which he/she is allowed access.
P.PHYSICAL	The information and information system resources (including media) are physically protected according to the sensitivity of the information processed, stored, or transmitted by the components.
P.PROTCTD_DOMAIN	The information system security functions maintain a separate protected security domain for their own execution. The components necessary for enforcing the security policies of the information system security functions shall maintain a security

	domain for their own execution that protects them from interference and tampering by other system activities and users.
P.RESIDUAL_DATA	All internal information system resources are cleared before reallocation of the resource to a different user.
P.RISKASSESS	Identification of system and environment vulnerabilities and an assessment of their impact on the system's security is regularly performed.
P.ROLE_SEPARATION	Security roles and responsibilities are distributed to preclude any one individual from adversely affecting operations or the integrity of the system.
P.SESSION_CTL	User access to a system is determined by the authenticated user's access profile.
P.SURVIVE	The system in conjunction with its environment must be resilient to insecurity, resisting the insecurity and/ or providing the means to detect an insecurity and recover from it.
P.SYS_ASSURANCE	The information system's security policy is maintained in the environment of distributed systems even if the systems are interconnected via an insecure networking medium (wire-lines, fiber, Internet, wireless, etc.).
P.SYS_RECOVERY	Controlled or trusted secure system recovery occurs in the event of an information system failure.
P.SYS_TESTING	Certification and post-accreditation testing is applied to the information system in accordance with PCSP and DAA requirements.
P.TRAINING	All users are trained to understand applicable system- use policies, the proper use of systems and the vulnerabilities inherent to those systems. This policy ensures that all users are properly instructed on policies and procedures for using the system, as well as, being able to acknowledge all threats and vulnerabilities that may impact system processing.
P.TRUSTED_USER	All users shall abide by designated policies and the conduct stated by those policies. In this context, 'users' includes both users of systems that interface with the TOE, and the administrators of systems that interface with the TOE in addition to the administrators of the TOE. This policy covers use and adherence to policies, procedures, system, admin, and user documentation, associated with the TOE and all systems that interface with the TOE.
P.UNIQUE_ID	Every authorized user of an information system is uniquely identified.

P.WARNING_BANNER	All authorized users are notified that they are subject to being monitored, recorded, and audited through the use of an NNSA approved warning text and positive acknowledgement by the user is required before granting the user access to system resources.
P.WFA	Waste Fraud and Abuse is detected or prevented and reported accordance with DOE O 221.1, Reporting Waste Fraud, and Abuse to the Office of IG.

4. Security Objectives

4.1 Security Objectives for the TOE

O.ACCESS_HISTORY	The information system user is notified upon successful logon of a) the date and time of the user's last logon, b) the location of the user (as can best be determined) at last logon, and c) the number of unsuccessful logon attempts using this user ID since the last successful logon. A positive action by the user is required to remove the notice.
O.ACCESS_MALICIOUS	Environmental controls are required to sufficiently mitigate (deterrence, detection, and response) the threat of malicious actions by authenticated users. Information system controls will help in achieving this objective, but will not be sufficient.
O.AUDIT_BASIC	The following activities must be recorded: • Successful use of the user security attribute administration functions; • All attempted uses of the user security attribute administration functions; and • Identification of which user security attributes have been modified. • With the exception of specific sensitive attribute data items (e.g., passwords, cryptographic keys); new values of the attributes should be captured. • Successful & unsuccessful logons and logoffs; • Unsuccessful access to security relevant files including creating, opening, closing, modifying, & deleting those files; • Changes in user authenticators; • Blocking or blacklisting user IDs, terminals, or access ports; • Denial of access for excessive logon attempts; and • Starting and ending times for each access to the system

O.AUDIT_FAILURE	An alternate audit capability or system shutdown must occur in the event of audit failure or when the audit trail exceeds 80% of capacity.
O.AUDIT_PROTECTION	The contents of audit trails must be protected against unauthorized access, modification, or deletion.
O.AUDIT_REVIEW	There must be a process for review of user activities and activities on behalf of the user on the TOE to detect and report actual or attempted circumvention of the TOE Security Functions (TSF).
O.AUTHENT_EXPOSE	The clear text display or exposure of any authenticator is only provided to the identified user during generation, issuance, storage, or use.
O.AUTHORIZATION	The TOE must ensure that only authorized users gain access to the information and TOE resources. The TOE must ensure for all actions under its control, except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access to subjects and objects.
O.CREDENTIAL_PROTECTION	Authentication credentials shall be protected like the information to which they provide access during creation, use, and handling.
O.DATA_CHANGES_DETERRED	Unauthorized changes to data in the information system are detected, deterred, and reported.
O.DETECT_HOST_BASIC	The information system environment, i.e., on-line, must provide the ability to detect low level, i.e., using methods readily available on the Internet to attack known vulnerabilities, attacks and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.
O.ENTRY_TOE	The information system must prevent logical entry to the information system using unsophisticated, technical methods, by persons without authority for such access.
O.ID_DISABLE	User TOE access is disabled when the user leaves the sponsoring organization, Access Authorization is terminated, loses authorized access (for cause, changes in organization, etc), or upon TOE detection of attempts to bypass security.
O.ID_REMOVAL	Prior to reuse of a user identifier, all previous access rights and privileges (including file accesses for that user identifier) are removed from the TOE
O.ID_REVALIDATION	User access, contact information, rights, and privileges, to include sponsor, Access Authorization, need-to-know, means for off line contact, mailing address, are validated annually.

O.INFO_FLOW	The information system and information system environment must ensure that any information flow control policies are enforced - (1) between system components and (2) at the system external interfaces.
O.INTEGRITY_LOW	The TOE will require user identification and authentication to validate the authority of the user for any changes to data.
O.MALICIOUS_CODE	The TOE must have the capability to detect and eliminate malicious code. Procedures to detect and deter incidents caused by malicious code are employed.
O.MANAGE_TOE	The information system must provide all the functions and facilities necessary to support the authorized administrators that are responsible for the management of information system security.
O.NTK_NNSA	Access rights to specific data objects are determined by object attributes assigned to that object, user identity, user attributes, and any formal access rights or privileges that NNSA has established for the data.
O.RECOVERY_CONTROLLED	Information system recovery is controlled via monitored terminal or system console.
O.RESIDUAL_PROTECTION	The information system must ensure that identified resources contain no residual data before being assigned, allocated, or reallocated.
O.RESOURCE_USAGE	The information system provides the capability to control a defined set of system resources (e. g., memory, and disk space) such that no one user can deny another user access to the resources.
O.ROLES_OTHER_SECURITY	Other roles involved with security administration, such as DBMS administration, are not performed by the same people performing the ISSO and system administrator roles.
O.SEC_FUNC_MANAGEMENT	The information system restricts management of information system security functions to authorized users.
O.SESSION_ESTABLISHMENT	The information system controls the establishment of sessions (a) by denying access after multiple (maximum of three) consecutive unsuccessful attempts on the same user ID; (b) by limiting the number of access attempts in a specified time period, (c) by use of a time-delay control system, or (d) by other such methods, subject to approval by the DAA
O.TRANS_SEC_UNCLAS	Information protection is required whenever Unclassified Protected or Unclassified Mandated Protection information is to be transmitted, carried to, or carried through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled

	electronic access to the information or communications media (e. g., outside the system perimeter). One or more of the following must be used: (a) Information distributed only within an area approved for open storage of the information; (b) National Security Agency (NSA)- approved type II encryption mechanisms; (c) DOE approved encryption mechanisms; or (d) NNSA approved protected transmission systems.
O.TRUSTED_PATH	The information system provides a trusted path between itself and the user for initial identification and authentication.
O.TSF_DOMAIN_SEPARATION	The information system maintains a domain for its own execution that protects it from external interference and tampering (e. g., by reading or modifying its code and data structures).
O.USER_INACTIVITY	The information system must detect an interval of user inactivity, such as no keyboard entries, and disable any future user activity until the user reestablishes the correct identity with a valid authenticator.
O.USER_LOCKING	The information system provides user initiated self-locking of interactive sessions. To unlock a user-locked session, the user must provide the correct identity with a valid authenticator.
O.WARNING_BANNER	All authorized users are notified that they are subject to being monitored, recorded, and audited through the use of an NNSA approved warning text and positive acknowledgement by the user is required before granting the user access to system resources.

4.2 Security Objectives for the Environment

O.ACCESS	Each user's access rights and privileges are authorized, prior to the user's first access to the TOE.
O.ACCESS_FORMAL	Prior to their first access to information, each user's need-to-know is formally authorized by management or the data owner-steward through a position description or written access list.
O.ACCESS_MALICIOUS	Environmental controls are required to sufficiently mitigate (deterrence, detection, and response) the threat of malicious actions by authenticated users. Information system controls will help in achieving this objective, but will not be sufficient.

O.AUTHORIZE_Non_TOE	The IT other than the information system must provide the ability to specify and manage user and system process access rights to individual processing resources and data elements under its control, supporting the organization's security policy for access control.
O.AVAILABILITY_LOW	Resources are provided to allow the information system user to perform data backup at the user's discretion.
O.CLEARING	The information system components and removable media are cleared before the items can be reused in another system environment with the same or different accreditation level as the original system components or removable media.
O.CREDENTIAL_PROTECTION	Authentication credentials shall be protected like the information to which they provide access during creation, use, and handling.
O.DATA_BACKUP_BASIC	User and information system data are available, or restorable, to meet mission availability requirements. Periodic checking of backup inventory and testing of the ability to restore information is accomplished to validate mission availability requirements are met.
O.DETECT_EXTERNAL_BASIC	The site environment, i.e., on-line, must provide the ability to detect low level, i.e., using methods readily available on the Internet to attack known vulnerabilities, attacks on the hosts and networks from outside the site and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.
O.DETECT_NETWORK_BASIC	The network environment, i.e., on-line, must provide the ability to detect low level, i.e., using methods readily available on the Internet to attack known vulnerabilities, attacks on the network and its components, and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.
O.DETECT_SITE_BASIC	The site environment, i.e., physical, must provide the ability to detect low level, i.e., using readily available methods to attack known vulnerabilities, attacks on the hosts and networks from inside the site and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.
O.ENTRY_NON_TECHNICAL	The information system environment must provide sufficient protection against non-technical attacks by other than authenticated users. User training and awareness will provide a major part of achieving this objective.
O.ENTRY_NON_TOE	For resources not controlled by the information system, IT other than the information system must prevent logical entry using unsophisticated, technical methods, by persons without authority for such access.

O.FORENSICS_PROC	Procedures are established and documented to ensure the identification, collection, and preservation of data needed to analyze penetration reconstruction, on-going cyber attacks and/ or failures
O.HARDWARE_EXAM_MINIMUM	Information system hardware components are examined for security impacts to the information system before use
O.ID_DISABLE	User TOE access is disabled when the user leaves the sponsoring organization, Access Authorization is terminated, loses authorized access (for cause, changes in organization, etc), or upon TOE detection of attempts to bypass security.
O.ID_REMOVAL	Prior to reuse of a user identifier, all previous access rights and privileges (including file accesses for that user identifier) are removed from the TOE
O.ID_REVALIDATION	User access, contact information, rights, and privileges, to include sponsor, Access Authorization, need-to-know, means for off line contact, mailing address, are validated annually.
O.INFO_FLOW	The information system and information system environment must ensure that any information flow control policies are enforced - (1) between system components and (2) at the system external interfaces.
O.INTEGRITY_LOW	The TOE will require user identification and authentication to validate the authority of the user for any changes to data.
O.MANAGE_TOE	The information system must provide all the functions and facilities necessary to support the authorized administrators that are responsible for the management of information system security.
O.MARK_COMPONENT	Each host, visual display, and output device will be marked with the sensitivity label (level) of the most sensitive Information Group the system is accredited to process, store, or transmit.
O.MARK_OUTPUT	All system output and removable media are appropriately marked with the level of the highest information sensitivity of the Information Groups that the system is accredited to operate with, or marked in with the sensitivity label for the information.
O.MEDIA_REVIEW	All media (paper, disks, zip drives, removable disk drives, etc.) are reviewed for classification and sensitivity and properly marked before release outside the system boundary.
O.NETWORK_INTERFACE	The developers of the information system must ensure the information system is not affected by the characteristics of the network(s) to which the information system is interfaced.

O.PHYS_MANDATED	Systems containing Unclassified Mandatory Protection information must be protected in one of the following ways: constantly attended or under the control of a person that possesses formal access approval and need to know; or protected in a manner described for Confidential or Critical Unclassified Information; or protected within locked rooms or buildings.
O.PHYSICAL	Physical attack that might compromise IT security on those parts of the information system critical to security is deterred and detected, primarily via prevention within the limits of COTS technology.
O.PHYSICAL_PROTECTION	The individuals responsible for the information system must ensure that the environment is capable of physically protecting the information system by signaling the occurrence of fire, flood, power loss, and environmental control failures that might adversely affect information system operations.
O.ROLES_OTHER_SECURITY	Other roles involved with security administration, such as DBMS administration, are not performed by the same people performing the ISSO and system administrator roles.
O.SOFTWARE_EXAM_MINIMUM	Information system software components are examined and tested for security impacts to the information system before use.
O.TRAINING	All users are trained to understand applicable information system-use policies, the approved use of the information system, and the vulnerabilities inherent in the operation of the information system.
O.TRANS_SEC_UNCLAS	Information protection is required whenever Unclassified Protected or Unclassified Mandated Protection information is to be transmitted, carried to, or carried through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e. g., outside the system perimeter). One or more of the following must be used: (a) Information distributed only within an area approved for open storage of the information; (b) National Security Agency (NSA)- approved type II encryption mechanisms; (c) DOE approved encryption mechanisms; or (d) NNSA approved protected transmission systems.
O.UNESCORT_ACCESS-UNCLASS	Access controls ensure that personnel granted unescorted physical access to the information, the information system or

human readable media have the appropriate formal access approvals and need-to-know.

5. IT Security Requirements

A MANDPP-conformant TOE may include information systems that are personal electronic devices, portable computers, and systems containing general-purpose operating systems, such as workstations, mainframes, or personal computers. These systems can be comprised of a single host or a set of cooperating hosts in a distributed system. Such systems permit one or more processors along with peripherals and storage devices to be used by single or multiple users to perform a variety of functions requiring access to the information stored on the system. The security functional and assurance requirements defined in this section must be applied to all elements in the TOE.

Some TOE components, where a single general user has the authority and responsibility to protect all general user data/information on the component (typically a single user desktop system) may be exempted from implementing these PP requirements with the approval of the cognizant Designated Approving Authority. Any TOE component where multiple general users may access data or share TOE resources must comply with the MANDPP requirements.

5.1 TOE Security Functional Requirements

This section defines the functional requirements for the TOE. Functional requirements components in this profile were drawn from Part 2 of the CC. Some functional requirements are extensions to those found in the CC.

CC defined operations for assignment, selection, and refinement were used to tailor the requirements to the level of detail necessary to meet the stated security objectives. These operations are indicated through the use of underlined (assignments and selections) and italicized (refinements) text. All required operations not performed within this profile are clearly identified and described such that they can be correctly performed upon instantiation of the PP into a Security Target (ST) specification.

NOTE: Where italicized items are listed in an assignment or selection clause in one of the following components, the ST developer must address the component and provide the information identified in the italicized clause. If the assignment or selection clause is not italicized, the item is mandatory and must be addressed in the ST.

5.1.1 FAU_ARP.1 Security alarms

5.1.1.1 FAU_ARP.1.1 The TSF shall take [assignment: *list of the least disruptive actions*] upon detection of a potential security violation.

Application Note: The ST must state the actions taken by the TOE when a potential security violation, such as detection of malicious code, or a successful or unsuccessful intrusion.

5.1.2 FAU_GEN.1 Audit data generation

5.1.2.1 FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- **Start-up and shutdown of the audit functions;**

- **All auditable events for the basic level of audit and the events listed below:**
  - **Successful use of the user security attribute administration functions**
  - **All attempted uses of the user security attribute administration functions**
  - **Identification of which user security attributes have been modified**
  - **Successful & unsuccessful logons and logoffs**
  - **Unsuccessful access to security relevant files including creating, opening, closing, modifying, & deleting those files**
  - **Changes in user authenticators**
  - **Blocking or blacklisting user Ids, terminals, or access ports**
  - **Denial of access for excessive logon attempts**
  - **System accesses by privileged users; a. Privileged activities at the system console (either physical or logical consoles) and other system- level accesses by privileged users.**
  - **Starting and ending times for each access to the system**

Application Note: For some situations it is possible that some events cannot be automatically generated. This is usually due to the audit functions not being operational at the time these events occur. Such events need to be documented in administrative guidance, along with recommendations on how manual auditing should be established to cover these events.

The "basic" level of auditing was selected as best representing the "mainstream" of contemporary audit practices used in the target environments.

5.1.2.2 **FAU_GEN.1.2** **The TSF shall record within each audit record at least the following iuformation:**

a. **Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and**

b. **For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information]**

5.1.3 FAU_GEN.2 User identity association

5.1.3.1 **FAU_GEN.2.1** **The TSF shall be able to associate each auditable event with the identity of the user that caused the event.**

Application Note: There are some auditable events that may not be associated with a user, such as failed login attempts. It is acceptable that such events do not include a user identity. In the case of failed login attempts it is also acceptable not to record the attempted identity in cases where that attempted identity could be misdirected authentication data; for example when the user may have been out of sync and typed a password in place of a user identifier.

5.1.4 FAU_SAA.1 Potential violation analysis

5.1.4.1 FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

5.1.4.2 FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

Accumulation or combination of [assignment: subset of defined auditable events] known to indicate a potential security violation; [assignment: any other rules].

Application Note: The ST must describe the auditable events that are known or suspected to indicate a potential security violation.

5.1.5 FAU_SAA.4 Complex attack heuristics

5.1.5.1 FAU_SAA.4.1 The TSF shall be able to maintain an internal representation of the following event sequences of known intrusion scenarios [assignment: list of sequences of system events whose occurrence are representative of known penetration scenarios] and the following signature events [assignment: *a subset of system events*] that may indicate a potential violation of the TSP.

Application Note: The ST must describe, or reference documentation of, known or suspected system events and penetration scenarios that may indicate a potential security violation. The specific manner of implementation is TOE dependent and can be achieved through the use of intrusion detection software on the TOE or in the local area network where the TOE is located.

5.1.5.2 FAU_SAA.4.2 The TSF shall be able to compare the signature events and event sequences against the record of system activity discernible from an examination of [assignment: *the information to be used to determine system activity*].

Application Note: See application note for FAU_SAA.4.1.

5.1.5.3 FAU_SAA.4.3 The TSF shall be able to indicate an imminent violation of the TSP when system activity is found to match a signature event or event sequence that indicates a potential violation of the TSP.

Application Note: See application note for FAU_SAA.4.1.

5.1.6 FAU_SAR.1 Audit review

5.1.6.1 FAU_SAR.1.1 The TSF shall provide [assignment: Computer System Security Officers (CSSO) and authorized system administrators] with the capability to read [assignment: all audit information] from the audit records.

Application Note: The minimum information that must be provided is the same that which is required to be recorded in FAU_GEN.1.2. The intent of this requirement is that there exists a tool for an administrator to access the audit trail in order to assess it. Exactly what manner is

provided is an implementation decision, but it needs to be done in a way that allows the administrator to make effective use of the information presented. This requirement is closely tied to FAU_SAR.3 and FAU_SEL.1. It is expected that a single tool will exist within the TSF that will satisfy all of these requirements.

5.1.6.2 FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.7 FAU_SAR.2 Restricted audit review

5.1.7.1 FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Application Note: By default, CSSOs and authorized system administrators may be considered to have been granted read access to the audit records. The TSF may provide a mechanism that allows other users to also read audit records.

5.1.8 FAU_SAR.3 Selectable audit review

5.1.8.1 FAU_SAR.3.1 The TSF shall provide the ability to perform [selection: searches, sorting, and ordering] of audit data based on based on the following attributes:

a. User identity;

b. [assignment: list of additional attributes that audit selectivity is based npon]

Application Note: The ST must state the additional attributes that audit selectivity may be based upon (e. g., object identity, type of event), if any.

5.1.9 FAU_SEL.1 Selective Audit

5.1.9.1 FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a. User identity;

b. [assignment: *list of additional attributes that audit selectivity is based upon*].

Application Note: The ST must state the additional attributes that audit selectivity may be based upon (e. g., object identity, type of event), if any.

5.1.10 FAU_STG.2 Guarantees of audit data availability

5.1.10.1 FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

5.1.10.2 FAU_STG.2.2 The TSF shall be able to [selection: prevent] modifications to the audit records.

Application Note: On many systems, in order to reduce the performance impact of audit generation, audit records will be temporarily buffered in memory before they are written to disk. In these cases, it is likely that some of these records will be lost if the operation of the TOE is interrupted by hardware or power failures. The developer needs to document what the likely loss will be and show that it has been minimized.

5.1.10.3 FAU_STG.2.3 The TSF shall ensure that [assignment: all audit records already written to media, i.e., not in memory buffers,] audit records will be maintained when the following conditions occur: [selection: audit storage exhaustion, failure, and attack]...

5.1.11 FAU_STG.3 Action in case of possible audit data loss

5.1.11.1 FAU_STG.3.1 The TSF shall [assignment: generate an alarm to the CSSO or authorized system administrator] if the audit trail exceeds [assignment: 80% of capacity].

Application Note: For this component, an "alarm" is to be interpreted as any clear indication to the administrator that the pre-defined limit has been exceeded. The ST author must state the pre-defined limit that triggers generation of the alarm. The limit can be stated as an absolute value, or as a value that represents a percentage of audit trail capacity (e. g., audit trail 80% full). If the limit is adjustable by the authorized administrator, the ST should also incorporate an FMT requirement to manage this function.

5.1.12 FAU_STG.4 Prevention of audit data loss

5.1.12.1 FAU STG.4.1 The TSF shall [selection: be able to prevent auditable events, except those taken by the CSSO or authorized system administrator,] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.

Application Note: The selection of "preventing auditable actions if audit storage is exhausted" is minimal functionality; providing a range of configurable choices (e. g., ignoring auditable actions and/ or changing to a degraded mode) is allowable, as long as "preventing" is one of the choices. If configurable, then FMT_ MOF.1 should be incorporated into the ST.

5.1.13 FCS_CKM.4 Cryptographic key destruction

5.1.13.1 FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

5.1.14 FCS_COP.1 Cryptographic operation

5.1.14.1 FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment:

***cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].**

5.1.15 FDP_ACC.2 Complete access control

5.1.15.1 FDP_ACC.2.1 **The TSF shall enforce the [assignment: Discretionary Access Control Policy (DAC)] on [assignment: list of subjects] acting on the behalf of users, [assignment: list of named objects] and all operations among subjects and objects covered by the SFP [DAC policy].**

Application Note: For most systems there is only one type of subject, usually called a process or task, which needs to be specified in the ST.

Named objects are those objects that are used to share information among subjects acting on the behalf of different users, and for which access to the object can be specified by a name or other identity. Any object that meets this criterion but is not controlled by the DAC policy must be justified.

The list of operations covers all operations between the above two lists. It may consist of a sublist for each subject-named object pair. Each operation needs to specify which type of access right is needed to perform the operation; for example read access or write access.

5.1.15.2 FDP_ACC.2.2 **The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.**

5.1.16 FDP_ACF.1 Security attribute based access control

5.1.16.1 FDP_ACF.1.1 **The TSF shall enforce the [assignment: Discretionary Access Control Policy] to objects based on [assignment: the following:]**

- **a. The user identity and group membership(s) associated with a subject;**
- **b. The following access control attributes associated with an object; and**
- **c. [assignment: List access control attributes. The attributes must provide permission attributes with:**
  - **a. the ability to associate allowed or denied operations with one or more user identities;**
  - **b. the ability to associate allowed or denied operations with one or more group identities; and**
  - **c. defaults for allowed or denied operations.**

5.1.16.2 FDP_ACF.1.2 **The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:**

[assignment: a set of rules specifying the Discretiouary Access Control policy, where:

a. **For each operation there shall be a rule, or rules, that use the permission attributes where the user identity of the subject matches a user identity specified in the access control attributes of the object;**

b. **For each operation there shall be a rule, or rules, that use the permission attributes where the group membership of the subject matches a group identity specified in the access control attributes of the object; and**

c. **For each operation there shall be a rule, or rules, which use the default permission attributes specified in the access control attributes of the object when neither a user identity nor group identity matches.]**

Application Note: A TOE that conforms to this PP is required to implement a DAC policy, but the rules that govern the policy may vary between TOEs; those rules need to be specified in the ST. In completing the rule assignment above, the resulting mechanism must be able to specify access rules that apply to at least any single user. This single user may have a special status such as the owner of the object. The mechanism must also support specifying access to the membership of at least any single group. Conformant implementations include self/ group/ public controls and access control lists.

A DAC policy may cover rules on accessing public objects; i.e., objects which are readable to all authorized users, but which can only be altered by the TSF or administrators. Specification of these rules should be covered under FDP_ACF.1.3 and FDP_ACF.1.4.

A DAC policy may include exceptions to the basic policy for access by administrators or other forms of special authorization. These rules should be covered under FDP_ACF.1.3.

The ST must list the attributes that are used by the DAC policy for access decisions. These attributes may include permission bits, access control lists, and object ownership.

A single set of access control attributes may be associated with multiple objects, such as all objects stored on a single floppy disk. The association may also be indirectly bound to the object, such as access control attributes being associated with the name of the object rather than directly to the object itself.

5.1.16.3 FDP_ACF.1.3 **The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].**

5.1.16.4 FDP_ACF.1.4 **The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].**

5.1.17 FDP_DAU.1 Basic data authentication

5.1.17.1 FDP_DAU.1.1 **The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: list of objects or information types].**

5.1.17.2 FDP_DAU.1.2 **The TSF shall provide [assignment: list of subjects] with the ability to verify evidence of the validity of the indicated information.**

5.1.18 FDP_IFC.1 Subset information flow control

5.1.18.1 FDP_IFC.1.1 **The TSF shall enforce the Discretionary Access Control Policy on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].**

5.1.19 FDP_IFF.1 Simple security attributes

5.1.19.1 FDP_IFF.1.1 **The TSF shall enforce the Discretionary Access Control Policy based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes].**

5.1.19.2 FDP_IFF.1.2 **The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].**

5.1.19.3 FDP_IFF.1.3 **The TSF shall enforce the [assignment: additional information flow control SFP rules].**

5.1.19.4 FDP_IFF.1.4 **he TSF shall provide the following [assignment: list of additional SFP capabilities].**

5.1.19.5 FDP_IFF.1.5 **The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows].**

5.1.19.6 FDP_IFF.1.6 **The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].**

5.1.20 FDP_ITC.1 Import of user data without security attributes

5.1.20.1 **FDP_ITC.1.1** **The TSF shall enforce the [assignment: discretionary Access Control Policy] when importing user data, controlled under the SFP, from outside of the TSC.**

5.1.20.2 FDP_ITC.1.2 **The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.**

5.1.20.3 FDP_ITC.1.3 **The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: *additional importation control rules*].**

5.1.21 FDP_RIP.1 Subset residual information protection

5.1.21.1 FDP_RIP.1.1 **The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource] to the following objects: [assignment: *list of objects*].**

Application Note: This requirement applies to the list of resources stated in the ST; it includes resources used to contain data and attributes. It also includes the encrypted representation of information.

Clearing the information content store of resources on deallocation from objects is sufficient to satisfy this requirement, if unallocated resources will not accumulate new information until they are allocated again.

5.1.22 FDP_SDI.2 Stored data integrity monitoring and action

5.1.22.1 FDP_SDI.2.1 **The TSF shall monitor user data stored within the TSC for [assignment: unauthorized modification and unauthorized deletion] on all objects, based on the following attributes: [assignment: *user data attributes*].**

Application Note: The ST must describe the user data attributes, i.e. file names, directory names, sizes, etc., that will be used in the detection of unauthorized activities on the data.

5.1.22.2 FDP_SDI.2.2 **Upon detection of a data integrity error, the TSF shall [assignment: enter a description of the error in the audit log and issue an alarm].**

Application Note: For this component, an "alarm" is to be interpreted as any clear indication to the administrator that a data integrity error has been detected. The ST must state the conditions that trigger generation of the alarm.

5.1.23 FIA_AFL.1 Authentication failure handling

5.1.23.1 FIA_AFL.1.1 **The TSF shall detect when [assignment: five (5) consecutive] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].**

Application Note: The ST must state the authentication events that will be monitored for 5 consecutive unsuccessful authentication attempts. The ST should also identify any authentication activities that are not monitored for unsuccessful authentication attempts.

5.1.23.2 FIA_AFL.1.2 **When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].**

5.1.24 FIA_ATD.1 User attribute definition

5.1.24.1 FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment:

a. **User Identifier;**
b. **Group Memberships;**
c. **Authentication Data;**
d. **Security-relevant Roles; and**
e. **[assignment: other user security attributes]].**

Application Note: The specified attributes are those that are required by the TSF to enforce the DAC policy, the generation of audit records, and proper identification and authentication of users. The user identity must be uniquely associated with a single individual user.

Group membership may be expressed in a number of ways: a list per user specifying to which groups the user belongs, a list per group which includes which users are members, or implicit association between certain user identities and certain groups. A TOE may have two forms of user and group identities, a text form and a numeric form. In these cases there must be unique mapping between the representations.

5.1.25 FIA_SOS.1 Verification of secrets

5.1.25.1 FIA_ SOS.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: the P_AUTHENTICATION policy].

Application Note: The P.AUTHENTICATION policy applies to all other information system users. The method of authentication is unspecified by this PP, but must be specified in the ST. The method that is used must be shown to implement the P.AUTHENTICATION policy. If a password mechanism is used, the mechanism must comply with NNSA password policies. The strength of whatever mechanism implemented must be subjected to strength of function analysis. (See AVA_SOF.1)

5.1.26 FIA_UAU.1 Timing of authentication

5.1.26.1 FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

Application Note: The ST must specify the actions that are allowed by an unauthenticated user. The allowed actions should be limited to those things that aid an authenticated user in gaining access to the TOE. This could include help facilities or the ability to send a message to administrators.

5.1.26.2 FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on the behalf of that user.

5.1.27 FIA_UAU.7 Protected authentication feedback

5.1.27.1 FIA_UAU.7.1 The TSF shall provide only [assignment: obscured feedback] to the user while the authentication is in progress.

Application Note: Obscured feedback implies the TSF does not produce a visible display of any authentication data entered by a user, such as through a keyboard (e. g., echo the password on the terminal). It is acceptable that some indication of progress be returned instead, such as a period returned for each character sent.

Some forms of input, such as card input based batch jobs, may contain human-readable user passwords. The administrative and user guidance documentation must explain the risks in placing passwords on such input and must suggest procedures to mitigate that risk.

5.1.27.2 FIA_UID.1 Timing of identification

5.1.27.3 FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

5.1.27.4 FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note: The ST must specify the actions that are allowed to an unidentified user. The allowed actions should be limited to those things that aid an authenticated user in gaining access to the TOE. This could include help facilities or the ability to send messages to administrators.

The method of identification is unspecified by this PP, but should be specified in a ST and it should specify how this relates to user identifiers maintained by the TSF.

5.1.28 FIA_USB.1 User-subject binding

5.1.28.1 FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

a. **The user identity which is associated with auditable events;**

b. **The user identity or identities which are used to enforce the Discretionary Access Control Policy;**

c. **The group membership or memberships used to enforce the Discretionary Access Control Policy;**

d. **[assignment: *any other user security attributes*].**

5.1.28.1.1 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of a user: [assignment: *changing of attributes rules*].

Application Note: The DAC policy and audit generation require that each subject acting on the behalf of users have a user identity associated with the subject. This identity is normally the one used at the time of identification to the system. The DAC policy enforced by the TSF may include provisions for making access decisions based on a user identity that differs from the one used during identification.

The ST must state, in FIA_USB.1.1, how this alternate identity is associated with a subject and justify why the individual user associated with this alternate identity is not compromised by the mechanism used to implement it. Depending on the TSF's implementation of group membership, the associations between a subject and groups may be explicit at the time of identification or implicit in a relationship between user and group identifiers. The ST must specify this association. Like user identification, an alternate group mechanism may exist, and parallel requirements apply.

5.1.29 FMT_MOF.1 Management of security functions behavior

5.1.29.1 FMT_MOF.1.1 The TSF shall restrict the ability to [selection: determine the behavior of, disable, enable, modify the behavior of] the functions [assignment: list of functions] to [assignment: CSSOs and authorized system administrators].

Application Note: The ST must state the restrictions and functions applied to the management of TOE security functions by the CSSO and authorized system administrators.

5.1.30 FMT_MSA.1 Management of security attributes

5.1.30.1 FMT_MSA.1.1 The TSF shall enforce the [assignment: Discretionary Access Control Policy] to restrict the ability to [selection: modify] the security attributes [assignment: access control attributes associated with a named object] to [assignment: the authorized users].

Application Note: The ST must state the components of the access rights that may be modified, and must state any restrictions that may exist for a type of authorized user and the components of the access rights that the user is allowed to modify. The ability to modify access rights must be restricted in that a user having access rights to a named object does not have the ability to modify those access rights unless explicitly granted the right to do so. This restriction may be explicit, based on the object ownership, or based on a set of object hierarchy rules.

5.1.31 FMT_MSA.2 Secure security attributes

5.1.31.1 FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.32 FMT_MSA.3 Static attribute initialization

5.1.32.1 FMT_MSA.3.1 The TSF shall enforce the [assignment: Discretionary Access Control Policy] to provide [selection: restrictive] default values for security attributes that are used to enforce the SFP [Discretionary Access Control Policy].

5.1.32.2 FMT_MSA.3.2 The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

Application Note: A TOE conforming to this PP must provide protection by default for all objects at creation time. This may be done through the enforcing of a restrictive default access control on newly created objects or by requiring the user to explicitly specify the desired access controls on the object at its creation. In either case, there shall be no window of vulnerability through which unauthorized access may be gained to newly created objects.

5.1.33 FMT_MTD.1 Management of TSF data

5.1.33.1 FMT_MTD.1.1 The TSF shall restrict the ability to [selection: create, delete, and clear] the [assignment: audit trail] to [assignment: CSSOs and authorized system administrators].

Application Note: The selection of "create, delete, and clear" functions for audit trail management reflect common management functions. These functions should be considered generic; any other audit administration functions that are critical to the management of a particular audit mechanism implementation should be specified in the ST.

5.1.33.1.1 The TSF shall restrict the ability to modify or observe the set of audited events to administrators.

Application Note: The set of audited events are the subset of auditable events that will be audited by the TSF. The term set is used loosely here and refers to the total collection of possible ways to control which audit records get generated; this could be by type of record, identity of user, identity of object, etc. It is an important aspect of audit that users are able to affect which of their actions are audited, and therefore must not have control over or knowledge of the selection of an event for auditing.

5.1.33.1.2 The TSF shall restrict the ability to initialize and modify the user security attributes, other than authentication data, to administrators.

Application Note: This component only applies to security attributes that are used to maintain the TSP. Other user attributes may be specified in the ST, but control of those attributes is not within the scope of this PP.

5.1.33.1.3 The TSF shall restrict the ability to modify the authentication data to the following:

a) administrators; and

b) users authorized to modify their own authentication data

Application Note: User authentication data refers to information that users must provide to authenticate themselves to the TSF. Examples include passwords, personal identification numbers, and fingerprint profiles. User authentication data does not include the user's identity. The ST must specify the authentication mechanism that makes use of the user authentication data to verify a user's identity. This component does not require that any user be authorized to modify their authentication information; it only states that it is permissible. It is not necessary that requests to modify authentication data require re-authentication of the requester's identity at the time of the request.

5.1.34 FMT_REV.1 Revocation

5.1.34.1 FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the [selection: users] within the TSC to [assignment: the CSSO and authorized system administrators].

5.1.34.2 FMT_REV.1.2 The TSF shall enforce the rules: [assignment:

a) The immediate revocation of security-relevant authorizations; and

b) [assignment: *list of other revocation rules concerning users*]].

Application Note: Many security-relevant authorizations could have serious consequences if misused, so an immediate revocation method must exist, although it need not be the usual method (e. g., The usual method may be editing the trusted users profile, but the change doesn't take effect until the user logs off and logs back on. The method for immediate revocation might be to edit the trusted users profile and "force" the trusted user to log off.). The immediate method must be specified in the ST and in administrator guidance. In a distributed environment the developer must provide a description of how the "immediate" aspect of this requirement is met.

The TSF shall restrict the ability to revoke security attributes associated with objects within the TSC to users authorized to modify the security attributes by the Discretionary Access Control policy.

5.1.34.3 FMT_REV.1.2 The TSF shall enforce the rules: [assignment:

a) The access rights associated with an object shall be enforced when an access check is made; and

b) [assignment: *list of other revocation rules concerning objects*]].

Application Note: The DAC policy may include immediate revocation (e. g., Multics immediately revokes access to segments) or delayed revocation (e. g., most UNIX systems do not revoke access to already opened files). The DAC access rights are considered to have been revoked when all subsequent access control decisions by the TSF use the new access control information. It is not required that every operation on an object make an explicit access control decision as long as a previous access control decision was made to permit that operation. It is sufficient that the developer clearly documents in guidance documentation how revocation is enforced.

5.1.35 FMT_SMR.2 Restrictions on security roles

5.1.35.1 FMT_SMR.2.1 The TSF shall maintain the roles: [assignment:

a) **CSSO;**
b) **administrator;**
c) **users authorized by the Discretionary Access Control Policy to modify object security attribntes;**
d) **users authorized to modify their own authentication data; and**
e) **[assignment: *other roles*]].**

Application Note: The ST must identify any other security relevant roles supported by the TOE.

5.1.35.2 FMT_SMR.2.2 The TSF shall be able to associate users with roles.

Application Note: A TOE conforming to this PP only needs to support a single administrative role, referred to as the administrator. If a TOE implements multiple independent roles, the ST should refine the use of the term administrators to specify which roles fulfill which requirements.

This PP specifies a number of functions that are required of or restricted to an administrator, but there may be additional functions that are specific to the TOE. This would include any additional function that would undermine the proper operation of the TSF. Examples of functions include: ability to access certain system resources like tape drives or vector processors, ability to manipulate the printer queues, and ability to run real-time programs.

5.1.35.3 FMT_SMR.2.3 The TSF shall ensure that the conditions [assignment: *conditions for the different roles*] are satisfied.

Application Note: If conditions or restrictions are applied to the different security relevant roles supported by the TOE, the conditions or restrictions must be stated in the ST.

5.1.36 FPT_AMT.1 Abstract machine testing

5.1.36.1 FPT_AMT.1.1 The TSF shall run a suite of tests [selection: *during initial start-up, periodically during normal operation, at the request of an authorized user, other conditions*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Application Note: In general this component refers to the proper operation of the hardware platform on which a TOE is running. The test suite needs to cover only aspects of the hardware on which the TSF relies to implement required functions, including domain separation. If a failure of some aspect of the hardware would not result in the TSF compromising the functions it performs, then testing of that aspect is not required.

5.1.37 FPT_ITC.1 Inter-TSF confidentiality during transmission

5.1.37.1 FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

Application Note: The ST must describe how the data is protected by one or more of the following:

a. Information distributed only within an area approved for open storage of the information;

b. National Nuclear Security Agency (NNSA)- approved encryption mechanisms appropriate for the encryption of unclassified mandatory protection information;

c. NNSA approved Protected Transmission System; and

d. Approved courier.

5.1.38 FPT_RVM.1 Reference Mediation

5.1.38.1 FPT_RVM.1.1 The TSF shall ensure that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Application Note: This element does not imply that there must be a reference monitor. Rather this requires that the TSF validate all actions between subjects and objects that require policy enforcement.

5.1.39 FPT_RCV.1 Manual recovery

5.1.39.1 FPT_RCV.1.1 After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

5.1.40 FPT_SEP.2 SFP domain separation

5.1.40.1 FPT_SEP.2.1 The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

5.1.40.2 FPT_SEP.2.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Application Note: This component does not imply a particular implementation of a TOE. The implementation needs to exhibit properties that the code and the data upon which TSF relies are not alterable in ways that would compromise the TSF and that observation of TSF data would not result in failure of the TSF to perform its job. This could be done either by hardware mechanisms or hardware architecture. Possible implementations include multi-state CPU's that support multiple task spaces and independent nodes within a distributed architecture. The second element can also be met in a variety of ways also, including CPU support for separate

address spaces, separate hardware components, or entirely in software. The latter is likely in layered application such as a graphic user interface system that maintains separate subjects.

5.1.40.3 FPT_SEP.2.3 The TSF shall maintain the part of the TSF related to [assignment: Discretionary Access Control policy] in a security domain for their own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to those SFPs.

5.1.41 FPT_STM.1 Reliable time stamps

5.1.41.1 FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Application Note: The generation of audit records depends on having a correct date and time. The ST needs to specify the degree of accuracy that must be maintained in order to maintain useful information for audit records.

5.1.42 FPT_TST.1 TSF testing

5.1.42.1 FPT_TST.1.1 The TSF shall run a suite of self-tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self test should occur]]* to demonstrate the correct operation of the TSF.

Application Note: In general this component refers to the proper operation of the TSF. The test suite needs to cover only aspects of the required functions of the TSF, including domain separation.

5.1.42.2 FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

5.1.42.3 FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

5.1.43 FRU_RSA.1 Maximum quotas

5.1.43.1 FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [assignment: controlled resources] that [selection: individual user, defined group of users, subjects] can use [selection: simultaneously, over a specified period of time].

5.1.44 FTA_MCS.1 Basic limitation on multiple concurrent sessions

5.1.44.1 FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

5.1.44.2 FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [assignment: one (1)] session per user.

5.1.45 FTA_SSL.1 TSF-initiated session locking

5.1.45.1 FTA_SSL.1.1 **The TSF shall lock an interactive session after [assignment: time interval of user inactivity] by:**

- **clearing or overwriting display devices, making the current contents unreadable;**
- **disabling any activity of the user's data access/display devices other than unlocking the session.**

5.1.45.2 FTA_SSL.1.2 **The TSF shall require the following events to occur prior to unlocking the session: [assignment:** events to occur**].**

5.1.46 FTA_SSL.2 User-initiated locking

5.1.46.1 FTA_SSL.2.1 **The TSF shall allow user-initiated locking of the user's own interactive session, by:**

a. **Clearing or overwriting display devices, making the current contents unreadable;**

b. **Disabling any activity of the user's data access/display devices other than unlocking the session.**

5.1.46.2 FTA_SSL.2.2 **The TSF shall require the following events to occur prior to unlocking the session: [assigument:** ***events to occur*****].**

Application Note: The ST must identify the events, if any, such as user authentication, necessary to unlock a session.

5.1.47 FTA_TAB.1 Default TOE access banners

5.1.47.1 FTA_TAB.1.1 **Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.**

Application Note: The warning banner must comply with the NNSA PCSP minimum banner or use an alternative banner wording approved by the organization's general counsel.

5.1.48 FTA_TAH.1 TOE access history

5.1.48.1 FTA_TAH.1.1 **Upon successful session establishment, the TSF shall display the [selection:** ***date, time, method, and location*****] of the last successful session establishment to the user.**

5.1.48.2 FTA_TAH.1.2 **Upon successful session establishment, the TSF shall display the [selection:** ***date, time, method, location*****] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.**

5.1.48.3 FTA_TAH.1.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

5.1.49 FTA_TSE.1 TOE session establishment

5.1.49.1 FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [assignment: *attributes*].

5.1.50 FTP_TRP.1 Trusted Path

5.1.50.1 FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: *remote, local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the commnnicated data from modification or disclosure.

5.1.50.2 FTP_TRP.1.2 The TSF shall permit [selection: *the TSF, local users, remote users*] to initiate communication via the trusted path.

5.1.50.3 FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial user authentication, [assignment: *other services for which trusted path is required*]].

5.2 TOE Security Assurance Requirements

On the following pages are the detailed assurance component requirements from a developer, content, and evaluator perspective. Also included are application notes:

5.2.1 Configuration Management

5.2.1.1 ACM_CAP.3 Authorization Controls

5.2.1.1.1 Developer action elements

ACM_CAP.1.1D The developer shall provide a reference for the TOE.

ACM_CAP.1.2D The developer shall provide a reference for the TOE.

ACM_CAP.1.3D The Developer shall use a Configuration Management (CM) System.

ACM_CAP.1.4D The developer shall use CM documentation.

5.2.1.1.2 Content and presentation of evidence elements

ACM_CAP.1.1C The reference for the TOE shall be unique to each version of the TOE

ACM_CAP.1.2C The TOE shall be labeled with its reference

ACM_CAP.1.3C The CM documentation shall include a configuration list and a CM plan.

ACM_CAP.1.4C **The configuration list shall describe the configuration items that comprise the TOE.**

ACM_CAP.1.5C **The CM documentation shall describe the method used to uniquely identify the configuration items.**

ACM_CAP.1.6C **The CM system shall uniquely identify all configuration items.**

ACM_CAP.1.7C **The CM shall describe how the CM system is used.**

ACM_CAP.1.8C **The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.**

ACM_CAP.1.9C **The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.**

ACM_CAP.1.10C **The CM system shall provide measures such that only authorized changes are made to the configuration items.**

5.2.1.1.3 Evaluator action elements

ACM_CAP.1.1E **The Evaluator shall confirm that the information provided meets all the requirements for the content & presentation of evidence.**

Application Note: This component provides three things. First it requires that the TOE is identifiable, using such things as version and part numbers, to ensure that the proper thing is installed. Second it requires that the pieces used to produce the TOE are identified. And third it requires that the production of the TOE be done in a controlled manner.

5.2.1.2 ACM_SCP.1 TOE CM Coverage

5.2.1.2.1 Developer action elements

ACM_SCP.1.1D **The developer shall provide CM documentation.**

5.2.1.3 Content and presentation of evidence elements

ACM_SCP.1.1C **The CM documentation shall show that the CM system, as a minimum, tracks the following: The TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.**

ACM_SCP.1.2C **The CM documentation shall describe how the configuration items are tracked by the CM system.**

5.2.1.4 Evaluator action elements

ACM_SCP.1.1E **The Evaluator shall confirm that the information provided meets all the requirements for the content & presentation of evidence.**

5.2.2 Delivery and Operation

5.2.2.1 ADO_DEL.1 Delivery Procedures

5.2.2.1.1 Developer action elements

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

5.2.2.2 Content and presentation of evidence elements

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the user's site.

5.2.2.3 Evaluator action elements

ADO_DEL.1.1E The Evaluator shall confirm that the information provided meets all the requirements for tbe content & presentation of evidence.

Application Note: The delivery procedures for the TOE can vary greatly and range from a shrink-wrapped box from a retail outlet to delivery by a field engineer. As such, there may be opportunities for third parties to tamper with the TOE delivery process. In these cases the developer should provide proven procedures or mechanisms to mitigate the threat.

5.2.2.4 ADO_IGS.1 Installation, generation, and startup procedures.

5.2.2.4.1 Developer action elements

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and startup of the TOE.

5.2.2.5 Content and presentation of evidence elements

ADO_IGS.1.1C The documentation shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.6 Evaluator action elements

ADO_IGS.1.1E The evaluator shall determine that the installation, generation and startup procedures result in a secure configuration.

Application Note: The required documentation depends on the way that the TOE is generated and installed. For example the generation of the TOE from source code may be done at the development site, in which case the required documentation would be considered part of the design documentation. On the other hand, if some part of the TOE generation is done by the TOE administrator, it would be part of the administrative guidance. Similar circumstances would apply to both installation and startup procedures.

5.2.3 Development

5.2.3.1 ADV_FSP.1 Informal functional specification

5.2.3.1.1 Developer action elements

ADV_FSP.1.1D The developer shall provide a functional specification.

5.2.3.1.2 Content and presentation of evidence elements

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions, and error messages as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

5.2.3.1.3 Evaluator action elements

ADV_FSP.1 .1E The evaluator shall confirm that the information provided meets all the requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete representation of the TOE security functional requirements.

Application Note: This component requires that the design documentation includes a complete external description of the TSF. In particular it needs to address the mechanisms that are used to meet the functional requirements of the PP. Other areas need to be addressed to the degree that they affect the functional requirements

5.2.3.2 ADV_HLD.2 Security enforcing high-level design.

5.2.3.2.1 Developer action elements

ADV_HLD.2.1D The developer shall provide the high level design of the TSF.

5.2.3.2.2 Content and presentation of evidence elements

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and / or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.7C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.8C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.9C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions, and error messages, as appropriate.

ADV_HLD.2.10C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

5.2.3.2.3 Evaluator action elements

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for the content and presentation of evidence.

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

Application Note: This component requires that the design documentation include a breakdown of the TSF at a very coarse grain. Both the developer and evaluator need to carefully choose how a subsystem is defined for a particular TOE. There must be a balance between subsystems being too large that is difficult to understand the functions of a single subsystem and subsystems that are so small that how they fit into the system as a whole is difficult to understand. If different pieces of the TSF are maintained by different groups of developers, that can aid in making these choices. Furthermore, it must be noted that the presentation need only be informal. This means that the interfaces between subsystems need be presented in general terms of how they interact, not to the level pf presenting a programming interface specification between them.

5.2.3.3 ADV_RCR.1 Representation correspondence

5.2.3.3.1 Developer action elements

ADV_RCR.1.1D The developer shall provide an analysis of the correspondence between all adjacent pairs of the TSF representations that are provided.

5.2.3.3.2 Content and presentation of evidence elements

ADV_RCR.1.1C For each adjacent pair of the provided TSF representations the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract representation.

5.2.3.3.3 Evaluator action elements

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for the content and presentation of evidence.

Application Note: For the PP, this ensures that the functional specifications and high-level design are consistent with each other.

5.2.3.4 ADV_SPM.1 Informal TOE security policy model

5.2.3.4.1 Developer action elements

ADV_SPM.1.1D **The developer shall provide a TSP model.**

ADV_SPM.1.2D **The developer shall demonstrate correspondence between the functional specification and the TSP model.**

5.2.3.4.2 Content and presentation of evidence elements

ADV_SPM.1.1C **The TSP model shall be informal.**

ADV_SPM.1.2C **The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.**

ADV_SPM.1.3C **The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.**

ADV_SPM.1.4C **The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.**

5.2.3.4.3 Evaluator action elements

ADV_SPM.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

5.2.4 Guidance Documents

5.2.4.1 AGD_ADM.1 Administrator Guidance

5.2.4.1.1 Developer action elements

AGD_ADM.1.1D **The developer shall provide administrator guidance addressed to system administrative personnel.**

5.2.4.1.2 Content and presentation of evidence elements

AGD_ADM.1.1C **The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.**

AGD_ADM.1.2C **The administrator guidance shall describe how to administer the TEO in a secure manner.**

AGD_ADM.1.3C **The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.**

AGD_ADM.1.4C **The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE**

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security relevant event relative to the administrative function that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall describe be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

5.2.4.1.3 Evaluator action elements

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for the content and presentation of evidence.

Application Note: The content required by this component is quite comprehensive and broadly stated: in particular the content needs to address any of the mechanisms and functions provided to the administrator to meet the functional requirements of the PP. It should also contain warnings about actions that may typically be done by administrators that should not be done on this specific TOE. This may include activating certain features or installing certain software that would compromise the TSF.

5.2.4.2 AGD_USR.1 User Guidance

5.2.4.2.1 Developer action elements

AGD_USR.1.1D The developer shall provide guidance

5.2.4.2.2 Content and presentation of evidence elements

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall contain warnings about user accessible functions and privileges that should be controlled in a secure processing euvironment.

AGD_USR.1.3C The user guidance shall clearly present all user responsibilities necessary for the secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of the TOE security environment. Note: this includes the securing of media, passwords, and etc.

AGD_USR.1.4C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.5C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

5.2.4.2.3 Evaluator action elements

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all

requirements for the content and presentation of evidence.

Application Note: The content required by this component is quite comprehensive and broadly stated: in particular the content needs to address any of the mechanisms and functions provided to the user to meet the functional requirements of the PP. It should also contain warnings about actions that may typically be done by users that should not be done on this specific TOE.

5.2.5 Life Cycle Support

5.2.5.1 AGD_USR.1 Development Security

5.2.5.1.1 Developer action elements

AGD_USR.1.1D The developer shall produce development security documentation.

5.2.5.1.2 Content and presentation of evidence elements

AGD_USR.1.1C The development security documentation shall describe all physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TEO design and implementation in its development environment.

AGD_USR.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

5.2.5.1.3 Evaluator action elements

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for the content and presentation of evidence

AGD_USR.1.2E The evaluator shall coufirm that the security measures are being applied

5.2.5.2 ALC_FLR.2 Flaw Reporting Procedures

5.2.5.2.1 Developer action elements

ALC_FLR.2.1 The developer shall provide flaw remediation procedures addressed to the TOE.

ALC_FLR.2.2D The developer shall establish a procedure for accepting aud acting upon user reports of security flaws and requests for correction of those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

5.2.5.2.2 Coutent aud presentation of evidence elements

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided as well as the status of finding a

correction to the flaw.

ALC_FLR.2.3C **The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.**

ALC_FLR.2.4C **The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections, and guidance on corrective actions to TOE users.**

ALC_FLR.2.5C **The flaw remediation procedures documentation shall describe a means by which the developer receives from the TOE users reports and inquiries of suspected security flaws in the TOE.**

ALC_FLR.2.6C **The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.**

ALC_FLR.2.7C **The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.**

ALC_FLR.2.8C **The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.**

5.2.5.2.3 Evaluator action elements

ALC_FLR.21.E **The evalnator shall confirm that the information provided meets all requirements for the content and presentation of evidence.**

5.2.6 Tests

5.2.6.1 ATE_COV.2 Analysis of coverage.

5.2.6.1.1 Developer action elements

ATE_COV.21.D **The developer shall provide an analysis of test coverage.**

5.2.6.1.2 Content and presentation of evidence elements

ATE_COV.2.1C **The analysis of test coverage shall demonstrate the correspondence between the test identified in the test documentation and the TSF as described in the functional specification.**

ATE_COV.2.2C **The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.**

5.2.6.1.3 Evaluator action elements

ATE_COV.21.E **The evaluator shall confirm that the information provided meets all requirements for the content and presentation of evidence.**

5.2.6.2 ATE_DPT.1 Testing: High-Level Design

5.2.6.2.1 Developer action elements

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

5.2.6.2.2 Content and presentation of evidence elements

ATE_DPT.1.1C The depth analysis shall demonstrate that the test identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

5.2.6.2.3 Evaluator action elements

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for the content and presentation of evidence.

Application Note: While the high-level design is used as the basis for testing, it is not required that internal interfaces between systems are tested.

5.2.6.3 ATE_FUN.1 Functional Testing

5.2.6.3.1 Developer action elements

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

5.2.6.3.2 Content and presentation of evidence elements

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results, and the actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedures shall identify the test to be performed and describe the scenarios for testing each security function. The scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.2.6.3.3 Evaluator action elements

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for the content and presentation of evidence.

5.2.6.4 ATE_IND.2 Independent Testing – Sample

5.2.6.4.1 Developer action elements

ATE_IND.2.1D The developer shall provide the TOE for testing.

5.2.6.4.2 Content and presentation of evidence elements

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.2.6.4.3 Evaluator action elements

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for the content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

Application Note: The choice of the subset to be tested and the sample of tests executed by the evaluator is entirely at the discretion of the evaluator.

5.2.7 Vulnerability Assessment

5.2.7.1 AVA_MSU.1 Examination of Guidance.

5.2.7.1.1 Developer action elements

AVA_MSU.1.1D The developer shall provide guidance documentation

5.2.7.1.2 Content and presentation of evidence elements

AVA_MSU.1.1C The guidance documentation shall identify all possible mode of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operations.

AVA_MSU.1.2C The guidance documentation shall be complete, clear, consistent, and reasonable.

AVA_MSU.1.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

5.2.7.1.3 Evaluator action elements

AVA_MSU.1.1E The evaluator shall confirm that the information provided meets all requirements for the content and presentation of evidence.

AVA_MSU.1.2E **The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.**

AVA_MSU.1.3E **The evaluator shall determiue that the use of the guidance documentation allows all insecure states to be detected.**

Application Note: This requirement can be approached as testing by the evaluator to ensure that the guidance documents are correct. The content elements primarily reinforce the guidance requirements themselves.

5.2.7.2 AVA_SOF.1 Strength of TOE security function evaluation.

5.2.7.2.1 Developer action elements

AVA_SOF.1.1D **The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.**

5.2.7.2.2 Content and presentation of evidence elements

AVA_SOF.1.1C **For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ ST.**

AVA_SOF.1.2C **For each mechanism with specific strength of TOE security functiou claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ ST.**

5.2.7.2.3 Evaluator action elements

AVA_SOF.1.1E **The evaluator shall confirm that the information provided meets all requirements for the content and presentation of evidence.**

AVA_SOF.1.2E **The evaluator shall confirm that the strength claims are correct.**

Application Note: The requirement applies to the authentication mechanism and any other mechanism that relies on its strength to ensure confidentiality and/ or integrity (e.g., encryption).

5.2.7.3 AVA_VLA.1 Developer vulnerability analysis

5.2.7.3.1 Developer action elements

AVA_VLA.1.1D **The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.**

AVA_VLA.1.2D **The developer shall document the disposition of the obvious vulnerabilities.**

5.2.7.3.2 Content and presentation of evidence elements

AVA_VLA.1.1C **The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.**

5.2.7.3.3 Evaluator action elements

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for the content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

Application Note: The evaluator should consider the following with respect to the search for obvious flaws:

a. dependencies among functional components and potential inconsistencies in the strength of unction among independent functions.

b. Potential inconsistencies between the TSP and the functional specification.

c. Potential gaps or inconsistencies in the HLD and potentially invalid assumptions about supporting hardware, software, or firmware required by the TSF.

d. Potential gaps in the administrator guidance that enable the administrator to fail: a) make effective use of TSF functions, b) to understands or take actions that need to be performed, c) to install and / or configure the TOE correctly, and, d) to avoid unintended interactions among security functions. In particular, Failure to describe all security parameters under the administrator's control and the effects of settings of those parameters.

e. Potential gaps in user guidance that enable the user to fail to control functions and privileges as required to maintain a secure processing environment. Potential presence in the user guidance of information that facilitates exploitation of vulnerabilities.

f. Open literature (e.g., CERT advisories, bug-trag mailing lists, etc.) that contains information on vulnerabilities on the TSF should be consulted.

5.3 Security Requirements for the IT Environment

The IT environment consists of those administrative processes to ensure Personnel Security, Communications Security, Physical Security, and Cyber Security requirements are met for the TOE as well as the adjudication of varying Cyber security requirements for interconnected systems or networks.

5.3.1 ENV_AMA.1 Malicious Access

5.3.1.1 ENV_AMA.1.1 Environmental controls are implemeuted to detect, deter, and respond to malicious actions by authenticated users.

Application Note: Intrusion detection by other components does not include electronic mail or electronic mail attachments that may execute malicious code upon opening.

5.3.2 ENV_AVA.1 Information Availability

5.3.2.1 ENV_AVA.1.1 **Capabilities and resources are provided to allow the information system user to perform data backup at the user's discretion.**

5.3.2.2 ENV_AVA.1.2 **User and information system data are available, or restorable, to meet mission availability requirements. Periodic checking of backup inventory and testing of the ability to restore information is accomplished to validate mission availability requirements are met.**

5.3.3 ENV_ATH.1 Management of User Identifiers and Authenticators

5.3.3.1 ENV_ ATH.1.1 **Authentication credentials shall be protected like the information to which they provide access during creation, use, and handling.**

5.3.3.2 ENV_ ATH.1.2 **Authenticated user TOE access is disabled when the user leaves the sponsoring organization, Access Authorization is terminated, loses authorized access (for cause, changes in organization, etc), or upon TOE detection of attempts to bypass security.**

5.3.3.3 ENV_ ATH.1.3 **Prior to reuse of an authenticated user identifier, all previous access rights and privileges (including file accesses for that user identifier) are removed from the TOE.**

5.3.3.4 ENV_ ATH.1.4 **Authenticated user access, contact information, rights, and privileges, to include sponsor, Access Authorization, need-to-know, means for off line contact, mailing address, are validated annually.**

5.3.4 ENV_CLR.1 Clearing

5.3.4.1 ENV_CLR.1.1 **The information system components and removable media are cleared before the items can be reused in another system environment with the same or different accreditation level as the original system components or removable media.**

5.3.5 ENV_EXM.1 Hardware and Software Examination

5.3.5.1 ENV_EXM.1.1 **Information system hardware components are examined for security impacts to the information system before use.**

5.3.5.2 ENV_EXM.1.2 **Information system software components are examined and tested for security impacts to the information system before use.**

5.3.6 ENV_FOR.1 Forensics

5.3.6.1 ENV_FOR.1.1 **Procedures are established and documented to ensure the identification, collection, and preservation of data needed to analyze penetration reconstruction, on-going cyber attacks and/ or failures**

5.3.7 ENV_IDS.1Intrusion Detection

5.3.7.1 ENV_IDS.1.1 **The site and network (when applicable) environment provides the ability to detect low level, i.e., using methods readily available on the Internet to attack known vnlnerabilities, attacks on the hosts and networks from outside the site and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.**

5.3.7.2 ENV_IDS.1.2 **The site and network (when applicable) environment provides the ability to detect low level, i.e., using readily available methods to attack known vulnerabilities, attacks on the hosts and networks from inside the site and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.**

5.3.7.3 ENV_IDS.1.3 **The network (when applicable) environment provides the ability to detect low level, i.e., using methods readily available on the Internet to attack known vulnerabilities, attacks on the network and its components, and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.**

5.3.8 ENV_INT.1 TOE Interface

5.3.8.1 ENV_INT.1.1 **The information system environment must ensure that any information flow control policies are enforced at the system (TOE) external interfaces.**

5.3.8.2 ENV_INT.1.2 **The developers of the information system must ensure that the information system security is not adversely affected by the characteristics of the network(s) to which the information system is interfaced.**

5.3.9 ENV_MRK.1 Marking

5.3.9.1 ENV_ MRK.1.1 **Each host, visual display, and output device will be marked with the sensitivity label (level) of the most sensitive Information Group the system is accredited to process, store, or transmit.**

5.3.9.2 ENV_MRK.1.2 **All system output is appropriately marked with the sensitivity label (level) of the highest sensitivity of the Information Groups that the system is accredited to operate with or with the sensitivity label for the information printed. All media (paper, disks, zip drives, removable disk drives, etc.) are reviewed for classification and sensitivity and properly marked before release outside the system boundary.**

5.3.10 ENV_NON.1 Non-TOE Access

5.3.10.1 ENV_NON.1.1 **The electronic environment in which the TOE resides (e.g. IT other than the information system) must provide the ability to specify and manage user access rights to the TOE processing and data resources (i.e. access authorization through the network), supporting the organization's security policy for access control.**

5.3.10.2 ENV_NON.1.2 **For resources not controlled by the information system, IT other than the information system must prevent logical entry using unsophisticated, technical methods, by persons without authority for such access.**

5.3.11 ENV_NOT.1 User Notification

5.3.11.1 ENV_NOT.1.1 **All users are notified that they are subject to being monitored, recorded, and audited through the use of an NNSA approved warning text and positive acknowledgement by the user is required before granting the user access to system resources.**

5.3.12 ENV_NTK.1 Need-To-Know

5.3.12.1 ENV_NTK.1.1 **Prior to their first access to information, each user's need-to-know is formally authorized by management or the data owner-steward.**

5.3.13 ENV_PHY.1 Physical Security

5.3.13.1 ENV_PHY.1.1 **Access controls ensure that personnel granted unescorted physical access to the information, the information system or human readable media have the appropriate formal access approvals and need-to-know.**

5.3.13.2 ENV_PHY.1.2 **Physical attack that might compromise IT security on those parts of the information system critical to security is deterred and detected.**

5.3.13.3 ENV_PHY1.3 **Systems containing [assignment: Unclassified Mandatory Protection information] shall, as a minimum, be protected by at least one of the following [assignment: constantly attended or under the control of a person that possesses proper authorization, formal access approval, and need to know; in a manner described for Unclassified Protected information; or in a manner to preclude unauthorized disclosure].**

5.3.14 ENV_PRO.1 Information Protection

5.3.14.1 ENV_PRO.1.1 **Information protection is required whenever [assignment: Unclassified Mandatory Protection] information is to be transmitted, carried to, or carried through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e. g., outside the system perimeter). One or more of [assignment:**

information distributed only within an area approved for open storage of the information; National Security Agency (NSA) - approved type II encryption mechanisms; doe approved encryption mechanisms; or NNSA approved protected transmission systems].

5.3.15 ENV_RCV.1 System Recovery

5.3.15.1 ENV_RCV.1.1 All remote terminal access must be monitored when used for system recovery operations.

5.3.16 ENV_REV.1 Media and Component Review

5.3.16.1 ENV_REV.1.1 All media (paper, disks, zip drives, removable disk drives, etc.) are reviewed for sensitivity and properly marked before release outside the system boundary.

5.3.17 ENV_RGT.1 User Access Rights and Privileges

5.3.17.1 ENV_ RGT.1.1 Each user's access rights and privileges are authorized, prior to the user's first access to the TOE.

5.3.18 ENV_ROL.1 Security Roles

5.3.18.1 ENV_ROL1.1 Other roles involved with security administration, such as DBMS administration, are not performed by the same people performing the ISSO and system administrator roles.

5.3.19 ENV_TNG.1 User Training

5.3.19.1 ENV_TNG.1.1 All authenticated users are trained to understand applicable information system-use policies, the approved use of the information system, aud the vulnerabilities inherent in the operation of the information system.

6. PP Application Notes

The Discretionary Access Control Policy, also referred to as DAC, is the basic policy that MANDPP compliant systems and products enforce over users and resources. Whether a user is granted a requested action, is determined by the TOE Security Policy (TSP) that is specified in this profile in the context of Discretionary Access Control (DAC). The DAC policy is the set of rules used to mediate user access to TOE protected objects and can be generally characterized as a policy which requires the TOE to allow authorized users and authorized administrators to control access to objects based on individual user identification. When the DAC policy rules are invoked, the TOE is said to be mediating access to TOE protected objects. However, there may be instances when the DAC policy is not invoked meaning that there may be objects residing in the TOE that are not protected by the TSP. In these instances the TOE is said to not be mediating access to a set of objects even though the TOE is executing a (possibly unauthorized) user request.

The DAC policy consists of two types of rules: those that apply to the behavior of authorized users (termed access rules) and those that apply to the behavior of authorized administrators (termed authorization rules). If an authorized user is granted a request to operate on an object, the user is said to have access to that object. There are numerous types of access; typical ones include read access and write access, which allow the reading and writing of objects respectively. If an authorized administrator is granted a requested service, the user is said to have authorization to the requested service or object. As for access, there are numerous possible authorizations. Typical authorizations include auditor authorization that allows an administrator to view audit records and execute audit tools and DAC override authorization that allows an administrator to override object access controls to administer the system.

7. Rationale

7.1 Security Objectives Rationale

Table 1. Policies, Threats, and Assumptions by Objective

Objective Name	Threat	Policy	Assumptions
O.ACCESS	T.ABUSE_OTHER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TOE, T.AUDIT_CONFIDENTIALITY_NON_TOE, T.ATTACK_OTHER, T.ENTRY_TOE, T.ENTRY_SOPHISTICATED, T.ERROR_USER, T.IMPERSON_OTHER, T.MASQUERADE_AUTHORIZED_USER, T.SPOOFING, T.SPRINGBOARD, T.STEGANOGRAPHY	P.PERSONNEL, P.AUTH_MGT, P.NTK	A.COOP
O.ACCESS_FORMAL	T.ABUSE_OTHER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ATTACK_OTHER, T.AUDIT_CONFIDENTIALITY_NON_TOE, T.ENTRY_TOE, T.ENTRY_SOPHISTICATED, T.ERROR_USER, T.IMPERSON_OTHER, T.MASQUERADE_AUTHORIZED_USER, T.SPOOFING, T.STEGANOGRAPHY	P.PERSONNEL, P.AUTH_MGT, P.NTK	A.COOP

Objective Name	Threat	Policy	Assumptions
O.ACCESS_HISTORY	T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ATTACK_OTHER, T.ENTRY_TOE, T.ENTRY_SOPHISTICATED, T.IMPERSON_OTHER, T.MASQUERADE_AUTHORIZED_USER, T.SPOOFING	P.ACCOUNTABILITY, P.MONITOR	
O.ACCESS_MALICIOUS	T.ACCESS_TOE, T.ACCESS_MALICIOUS, T.ATTACK_OTHER, T.IMPERSON_OTHER, T.MASQUERADE_AUTHORIZED_USER, T.PHYSICAL, T.SPOOFING, T.SYSTEM_CORRUPTED, T.TOE_CORRUPTED	P.PERSONNEL, P.AUTH_MGT, P.NTK	A.COOP

Objective Name	Threat	Policy	Assumptions
O.AUDIT_BASIC	T.ABUSE_ADMIN, T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TECHNICAL, T.ACCESS_NON_TOE, T.ERROR_ADMIN, T.ATTACK_OTHER, T.AUDIT_CONFIDENTIALITY_TOE , T.CONSUME_OTHER, T.ENTRY_TOE, T.ENTRY_NON_TECHNICAL, T.ENTRY_SOPHISTICATED, T.ERROR_USER, T.FLAWED_CODE, T.IMPERSON_OTHER, T.MASQUERADE_AUTHORIZED_U SER, T.NON_REPUDIATION_RECIEVE, T.NON_REPUDIATION_SEND, T.NON_REPUDIATION_TRANSAC TION, T.OPERATE, T.RECORD-EVENT_TOE, T.RECORD_NON_TOE, T.SPOOFING, T.SPRINGBOARD, T.TAMPER, T.TRACEABLE_TOE, T.TRAPDOOR_BENIGN_ADMIN	P.ACCOUNTABILITY, P.MONITOR, P.FORENSICS, P.UNIQUE_ID	

Objective Name	Threat	Policy	Assumptions
O.AUDIT_FAILURE	T.ABUSE_ADMIN, T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TECHNICAL, T.ACCESS_NON_TOE, T.AUDIT_CORRUPTED_TOE, T.ENTRY_NON_TECHNICAL, T.OPERATE, T.RECORD-EVENT_TOE, T.RECORD_EVENT_NON_TOE, T.SPRINGBOARD	P.ACCOUNTABILITY, P.MONITOR, P.FORENSICS	
O.AUDIT_PROTECTION	T.ABUSE_ADMIN, T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TECHNICAL, T.ACCESS_NON_TOE, T.ERROR_ADMIN, T.ATTACK_OTHER, T.AUDIT_CONFIDENTIALITY_TOE , T.AUDIT_CONFIDENTIALITY_NO N_TOE, T.AUDIT_CORRUPTED_TOE, T.CONSUME_OTHER, T.ENTRY_TOE, T.ENTRY_NON_TECHNICAL, T.ENTRY_SOPHISTICATED, T.ERROR_USER, T.FLAWED_CODE, T.IMPERSON_OTHER, T.MASQUERADE_AUTHORIZED_U SER, T.RECORD_EVENT_TOE, T.RECORD_EVENT_NON_TOE, T.SPOOFING, T.TRACEABLE_TOE, T.TRAPDOOR_BENIGN_ADMIN	P.ACCOUNTABILITY, P.MONITOR, P.FORENSICS	A.COOP

Objective Name	Threat	Policy	Assumptions
O.AUDIT_REVIEW	T.ABUSE_ADMIN, T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TECHNICAL, T.ACCESS_NON_TOE, T.ERROR_ADMIN, T.ATTACK_OTHER, T.AUDIT_CONFIDENTIALITY_TOE, T.CONSUME_OTHER, T.ENTRY_TOE, T.ENTRY_NON_TECHNICAL, T.ENTRY_SOPHISTICATED, T.IMPERSON_OTHER, T.MASQUERADE_AUTHORIZED_USER, T.NON_REPUDIATION_RECIEVE, T.NON_REPUDIATION_SEND, T.NON_REPUDIATION_TRANSACTION, T.OPERATE, T.RECORD_EVENT_TOE, T.RECORD_EVENT_NON_TOE, T.SPOOFING, T.SPRINGBOARD, T.TAMPER, T.TRACEABLE_TOE, T.TRAPDOOR_BENIGN_ADMIN	P.ACCOUNTABILITY, P.MONITOR, P.FORENSICS	
O.AUTHENT_EXPOSE	T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TECHNICAL, T.IMPERSON_OTHER, T.LINK_OTHER	P.NTK, P.ACCOUNTABILITY, P.AUTH_MGMT, P.DATA_AVAILABILITY	
O.AUTHORIZATION	T.SPRINGBOARD	P.NTK, P.UNIQUE_ID	A.COOP

Objective Name	Threat	Policy	Assumptions
O.AUTHORIZE_Non_TOE:	T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.OPERATE, T.SPRINGBOARD	P.COMPOSITION	A.COOP
O.AVAILABILITY_HIGH	T.CRASH, T.MAINTENANCE	P.ALT_INFRASTRUCTURE, P.CONOPS, P.DATA_AVAILABILITY, P.SURVIVE	
O.AVAILABILITY_LOW	T.CRASH, T.MAINTENANCE	P.ALT_INFRASTRUCTURE, P.CONOPS, P.DATA_AVAILABILITY, P.SURVIVE	
O.CLEARING	T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_MALICIOUS, T.ACCESS_NON_TECHNICAL, T.ACCESS_NON_TOE, T.ENTRY_NON_TECHNICAL, T.INTENTIONAL_DISCLOSURE, T.MASQUERADE_AUTHORIZED_USER, T.OPERATE, T.SECRET_OTHER, T.UNINTENTIONAL_DISCLOSURE	P.RESIDUAL_DATA, P.NTK	
O.CREDENTIAL_PROTECTION	T.LINK_OTHER, T.SPRINGBOARD	P.CREDENTIAL_PROTECTION	

Objective Name	Threat	Policy	Assumptions
O.DATA_BACKUP_BASIC	T.ABUSE_ADMIN, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TOE, T.ERROR_ADMIN, T.ATTACK_OTHER, T.AUDIT_CORRUPTED_NON_TOE, T.AUDIT_CORRUPTED_TOE, T.CRASH, T.DELETE_UNINTENTIONAL, T.ENTRY_TOE, T.INTEGRITY_OTHER, T.MAINTENANCE, T.MALICIOUS_CODE, T.MODIFY_OTHER, T.OPERATE, T.PHYSICAL_ATTACK, T.RECORD_EVENT_TOE, T.SABOTAGE_DATA/ SOFTWARE, T.SYSTEM_CORRUPTED	P.DATA_AVAILABILITY, P.SURVIVE, P.SYS_RECOVERY	
O.DATA_CHANGES_DETERRED	T.ABUSE_ADMIN, T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ERROR_ADMIN, T.ATTACK_OTHER, T.ERROR_USER, T.INTEGRITY_OTHER, T.MODIFY_OTHER, T.NON_REPUDIATION_TRANSACTION, T.OPERATE, T.SABOTAGE_DATA/ SOFTWARE, T.SPOOFING, T.UNAUTHORIZED_MALICIOUS_SOFTWARE	P.DATA_ASSURANCE	

Objective Name	Threat	Policy	Assumptions
O.DETECT_EXTERNAL_BASIC	T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TECHNICAL, T.ACCESS_NON_TOE, T.ATTACK_OTHER, T.CAPTURE, T.CONSUME_OTHER, T.EAVESDROPPING, T.ENTRY_NON_TOE, T.ENTRY_TOE, T.ENTRY_SOPHISTICATED, T.FLAWED_CODE, T.IMPERSON_OTHER, T.MASQUERADE_AUTHORIZED_USER, T.OPERATE, T.RECORD_EVENT_NON_TOE, T.SPOOFING, T.SPRINGBOARD, T.SYSTEM_CORRUPTED, T.TAMPER, T.TRAPDOOR_MALICIOUS_SOFTWARE	P.IDS	

Objective Name	Threat	Policy	Assumptions
O.DETECT_HOST_BASIC	T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TECHNICAL, T.ACCESS_NON_TOE, T.ATTACK-OTHER, T.CAPTURE, T.CONSUME_OTHER, T.EAVESDROPPING, T.ENTRY_NON_TOE, T.ENTRY_TOE, T.ENTRY_SOPHISTICATED, T.ERROR_USER, T.FLAWED_CODE, T.OPERATE, T.RECORD_EVENT_NON_TOE, T.SPOOFING, T.SPRINGBOARD, T.SYSTEM_CORRUPTED, T.TAMPER, T.TRAPDOOR_MALICIOUS_SOFTWARE	P.IDS	

Objective Name	Threat	Policy	Assumptions
O.DETECT_NETWORK_BASIC	T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TECHNICAL, T.ACCESS_NON_TOE, T.ATTACK_OTHER, T.CAPTURE, T.CONSUME_OTHER, T.EAVESDROPPING, T.ENTRY_NON_TOE, T.ENTRY_TOE, T.ENTRY_SOPHISTICATED, T.ERROR_USER, T.FLAWED_CODE, T.MASQUERADE_AUTHORIZED_USER, T.OPERATE, T.RECORD_EVENT_NON_TOE, T.SPOOFING, T.SYSTEM_CORRUPTED, T.TAMPER	P.IDS	

Objective Name	Threat	Policy	Assumptions
O.DETECT_SITE_BASIC	T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TECHNICAL, T.ACCESS_NON_TOE, T.ATTACK_OTHER, T.CAPTURE, T.CONSUME_OTHER, T.EAVESDROPPING, T.ENTRY_NON_TOE, T.ENTRY_TOE, T.ENTRY_SOPHISTICATED, T.ERROR_USER, T.FLAWED_CODE, T.IMPERSON_OTHER, T.MASQUERADE_AUTHORIZED_USER, T.OPERATE, T.RECORD_EVENT_NON_TOE, T.SPOOFING, T.SPRINGBOARD, T.SYSTEM_CORRUPTED, T.TAMPER, T.TRAPDOOR_MALICIOUS_SOFTWARE	P.IDS	
O.ENTRY_NON_TECHNICAL	T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TECHNICAL, T.ACCESS_NON_TOE, T.MASQUERADE_AUTHORIZED_USER, T.OPERATE	P.PHYSICAL P.NTK	A.COOP
O.ENTRY_Non_TOE	T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TECHNICAL, T.IMPERSON_OTHER, T.LINK_OTHER	P.COMPOSITION	A.COOP

Objective Name	Threat	Policy	Assumptions
O.ENTRY_TOE	T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.MASQUERADE_AUTHORIZED_USER	P.NTK, P.MALICIOUS_CODE	A.COOP
O.FORENSICS_PROC	T.ABUSE_ADMIN, T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TECHNICAL, T.AUDIT_CORRUPTED_NON_TOE, T.ERROR_ADMIN, T.ATTACK_OTHER, T.ERROR_USER, T.IMPERSON_OTHER, T.RECORD_EVENT_TOE, T.TAMPER, T.TRACEABLE_TOE, T.TRAPDOOR_BENIGN_ADMIN, T.TRAPDOOR_MALICIOUS_CODE	P.FORENSICS	
O.HARDWARE_EXAM_MINIMUM	T.INSTALL, T.SYSTEM_CORRUPTED, T.TAMPER	P.CONFIG_MGMT, P.MALICIOUS_CODE, P.DUE_CARE	A.PROTECT
O.ID_DISABLE	T.ABUSE_ADMIN, T.ABUSE_OTHER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ERROR_ADMIN, T.ENTRY_SOPHISTICATED, T.IMPERSON_OTHER, T.MASQUERADE_AUTHORIZED_USER, T.OPERATE, T.SPOOFING	P.NTK, P.DENY_ACCESS	

Objective Name	Threat	Policy	Assumptions
O.ID_REMOVAL	T.ABUSE_ADMIN, T.ABUSE_OTHER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ENTRY_SOPHISTICATED, T.IMPERSON_OTHER, T.MASQUERADE_AUTHORIZED_USER, T.OPERATE, T.SPOOFING	P.NTK, P.DENY_ACCESS	
O.ID_REVALIDATION	T.ABUSE_ADMIN, T.ACCESS_TOE, T.ERROR_ADMIN, T.IMPERSON_OTHER	P.UNIQUE_ID, P.DENY_ACCESS	
O.INFO_FLOW	T.ABUSE_OTHER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TOE, T.ENTRY_SOPHISTICATED, T.LOSS_SOFTWARE, T.SYSTEM_CORRUPTED, T.TAMPER, T.TRAPDOOR_MALICIOUS_SOFTWARE	P.NTK, P.CTL_INTERFACE, P.COMPOSITION, P.INFO_FLOW,	A.PEER
O.INTEGRITY_LOW	T.ABUSE_ADMIN, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_MALICIOUS, T.ERROR_ADMIN, T.ATTACK_OTHER, T.INTEGRITY_OTHER, T.MODIFY_OTHER, T.OPERATE, T.UNAUTHORIZED_MALICIOUS_SOFTWARE	P.DATA_ASSURANCE, P.NTK	A.COOP

Objective Name	Threat	Policy	Assumptions
O.MALICIOUS_CODE	T.ABUSE_ADMIN, T.ABUSE_OTHER, T.ACCESS_TOE, T.ERROR_ADMIN, T.INSTALL, T.MALICIOUS_CODE, T.OPERATE, T.TRAPDOOR_MALICIOUS_CODE, T.UNAUTHORIZED_MALICIOUS_SOFTWARE	P.MALICIOUS_CODE	A.PROTECT
O.MANAGE_TOE	T.ABUSE_ADMIN, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.AUTHENTICATION_NETWORK, T.ENTRY_SOPHISTICATED, T.FAILURE_DISTRIBUTED_SYS_COMPONENT, T.OPERATE, T.TAMPER		
O.MARK_COMPONENT	T.ACCESS_NON_TECHNICAL, T.INTENTIONAL_DISCLOSURE, T.SECRET_OTHER	P.MEDIA_MARKING, P.FILE_REVIEW, P.MEDIA_REVIEW, P.NTK	
O.MARK_OUTPUT	T.ABUSE_USER, T.ACCESS_NON_TECHNICAL, T.EXPORT, T.INTENTIONAL_DISCLOSURE, T.OPERATE, T.SECRET_OTHER, T.UNINTENTIONAL_DISCLOSURE, T.STEGANOGRAPHY	P.MEDIA_MARKING, P.FILE_REVIEW, P.MEDIA_REVIEW, P.NTK	
O.MEDIA_REVIEW	T.ACCESS_TOE, T.ACCESS_NON_TECHNICAL, T.EXPORT, T.INTENTIONAL_DISCLOSURE, T.SECRET_OTHER, T.UNINTENTIONAL_DISCLOSURE, T.STEGANOGRAPHY	P.MEDIA_MARKING, P.FILE_REVIEW, P.MEDIA_REVIEW, P.NTK	

Objective Name	Threat	Policy	Assumptions
O.NETWORK_INTERFACE	T.EAVESDROPPING, T.INSTALL, T.SPRINGBOARD, T.SYSTEM_CORRUPTED, T.TAMPER, T.TOE_CORRUPTED	P.COMPOSITION, P.CTL_INTERFACE	A.PEER
O.NTK_NNSA	T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TOE, T.ENTRY_TOE, T.ENTRY_SOPHISTICATED, T.INTENTIONAL_DISCLOSURE, T.SPRINGBOARD, T.TAMPER	P.NTK	A.COOP
O.PHYS_MANDATED	T.ACCESS_NON_TECHNICAL, T.ENTRY_NON_TECHNICAL, T.INTENTIONAL_DISCLOSURE, T.MASQUERADE_AUTHORIZED_USER, T.OBSERVE_OTHER, T.PHYSICAL, T.PHYSICAL_ATTACK, T.SABOTAGE_DATA/ SOFTWARE, T.SPOOFING, T.SYSTEM_CORRUPTED, T.TAMPER, T.TOE_CORRUPTED	P.PHYSICAL	
O.PHYSICAL	T.ACCESS_NON_TECHNICAL, T.ENTRY_NON_TECHNICAL, T.INSTALL, T.PHYSICAL, T.PHYSICAL_ATTACK, T.SABOTAGE_DATA/ SOFTWARE, T.SPOOFING, T.SYSTEM_CORRUPTED, T.TAMPER, T.TOE_CORRUPTED	P.PHYSICAL	A.CONNECT, A.LOCATE, A.PROTECT
O.PHYSICAL_PROTECTION	T.ACCESS_NON_TECHNICAL, T.ENTRY_NON_TECHNICAL, T.PHYSICAL_ATTACK, T.SABOTAGE_DATA/ SOFTWARE	P.PHYSICAL	

Objective Name	Threat	Policy	Assumptions
O.RECOVERY_CONTROLLED	T.CRASH, T.TOE_CORRUPTED	P.SYS_RECOVERY	
O.RESIDUAL_PROTECTION	T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.LINK_OTHER, T.MASQUERADE_AUTHORIZED_USER, T.OPERATE, T.SECRET_OTHER	P.RESIDUAL_DATA, P.NTK	
O.RESOURCE_USAGE	T.DENY_OTHER, T.OPERATE	P.DATA_AVAILABILITY	
O.ROLES_OTHER_SECURITY	T.ABUSE_ADMIN, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ATTACK_OTHER, T.AUDIT_CORRUPTED_TOE, T.CONFIGURATION_ADMIN, T.OPERATE	P.ROLE_SEPARATION	
O.SEC_FUNC_MANAGEMENT	T.SPRINGBOARD, T.TAMPER	P.NTK, P.ROLE_SEPARATION	
O.SESSION_ESTABLISHMENT	T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ENTRY_OTHER, T.SPRINGBOARD, T.ENTRY_TOE	P.SESSION_CTL	A.COOP
O.SOFTWARE_EXAM_MINIMUM	T.FLAWED_CODE, T.INSTALL, T.SYSTEM_CORRUPTED, T.TOE_CORRUPTED, T.TRAPDOOR_MALICIOUS_CODE	P.COMPOSITION, P.MALICIOUS_CODE	A.PROTECT

Objective Name	Threat	Policy	Assumptions
O.TRAINING	T.ABUSE_ADMIN, T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_TOE, T.ACCESS_UNDETECTED, T.ACCESS_MALICIOUS, T.ACCESS_NON_TECHNICAL, T.ERROR_ADMIN, T.DELETE_UNINTENTIONAL, T.MASQUERADE_AUTHORIZED_USER, T.OBSERVE_TOE, T.OBSERVE_NON_TOE, T.SOCIAL_ENGINEERING, T.TRAPDOOR_BEGIN_ADMIN, T.UNAUTHORIZED_MALICIOUS_SOFTWARE, T.UNINTENTIONAL_MALICIOUS_SOFTWARE, T.UNINTENTIONAL_DISCLOSURE	P.TRAINING, P.RISK_ASSESS, P.DUE_CARE, P.SURVIVE, P.TRUSTED_USER, P.WFA	A.TRAINED_ADM, A.MANAGE
O.TRANS_SEC_UNCLASS	T.ACCESS_TOE, T.ACCESS_MALICIOUS, T.CAPTURE, T.EAVESDROPPING, T.LINK_OTHER, T.MASQUERADE_AUTHORIZED_USER, T.PHYSICAL, T.SECRET_OTHER	P.CRYPTOGRAPY, P.NTK, P.DATA_ASSURANCE, P.SYS_ASSURANCE	
O.TRUSTED_PATH	T.ACCESS_TOE, T.AUTHENTICATION_NETWORK	P.NTK, P.SYS_ASSURANCE, P.ACCOUNTABILITY, P.CREDENTIAL_PROTECTION, P.STRONG_AUTHENTICATION	
O.TSF_DOMAIN_SEPARATION	T.AUDIT_CORRUPTED_NON_TOE, T.AUDIT_CORRUPTED_TOE, T.CONFIDENTIALITY_NON_TOE, T.CONFIDENTIALITY_TOE	P.SYS_ASSURANCE, P.PROTCTD_DOMAIN	
O.UNESCORT_ACCESS_UNCLASS	T.MASQUERADE_AUTHORIZED_USER, T.OBSERVE_OTHER, T.UNINTENTIONAL_DISCLOSURE, T.PHYSICAL	P.NTK, P.PHYSICAL, P.CONFIG_MGMT, P.DATA_AVAILABILITY, P.PERSONNEL,	A.COOP

Objective Name	Threat	Policy	Assumptions
O.USER_INACTIVITY	T.ACCESS_TOE, T.INSTALL, T.MASQUERADE_AUTHORIZED_USER, T.SECRET_OTHER, T.SPRINGBOARD	P.NTK, P.ACCOUNTABILITY, P.KNOWN, P.DENY_ACCESS, P.DUE_CARE, P.DATA_ASSURANCE	
O.USER_LOCKING	T.ACCESS_TOE, T.INSTALL, T.MASQUERADE_AUTHORIZED_USER, T.SECRET_OTHER, T.SPRINGBOARD,	P.NTK, P.ACCOUNTABILTY, P.KNOWN, P.DENY_ACCESS, P.DUE_CARE, P.DATA_ASSURANCE	
O.WARNING_BANNER	T.ABUSE_ADMIN, T.ABUSE_OTHER, T.ABUSE_USER, T.ACCESS_TOE, T.ATTACK-OTHER, T.ENTRY_TOE, T.ENTRY_SOPHISTICATED, T.OPERATE	P.WFA, P.WARNING_BANNER	

7.2 Security Requirements Rationale

Table 2. Functional Components Implementing Objectives

Objective	Functional Component
O.ACCESS	ENV_RGT.1
O.ACCESS_FORMAL	ENV_NTK.1
O.ACCESS_HISTORY	FTA_TAH.1
O.ACCESS_MALICIOUS	FIA_SOS.1, ENV_AMA.1
O.AUDIT_BASIC	FAU_GEN.1, FAU_GEN.2, FAU_SEL.1, FPT_TST.1, FPT_AMT.1, FPT_STM.1
O.AUDIT_FAILURE	FAU_STG.3, FAU_STG.4
O.AUDIT_PROTECTION	FAU_SAR.2, FAU_STG.2, FPT_TST.1
O.AUDIT_REVIEW	FAU_SAA.1, FAU_SAR.1, FAU_SAR.3
O.AUTHENT_EXPOSE	FIA_UAU.7
O.AUTHORIZATION	FDP_ACC.2, FDP_ACF.1, FIA_ATD.1, FIA_UAU.1, FIA_UID.1, FPT_TST.1
O.AUTHORIZE_Non_TOE:	ENV_NON.1
O.AVAILABILITY_LOW	ENV_RCV.1
O.CLEARING	ENV_CLR.1
O.CREDENTIAL_PROTECTION	FIA_UAU.7, FMT_MTD.1, ENV_ATH.1
O.DATA_BACKUP_BASIC	ENV_AVA.1
O.DATA_CHANGES_DETERRED	FDP_DAU.1, FDP_SDI.2
O.DETECT_EXTERNAL_BASIC	ENV_IDS.1
O.DETECT_HOST_BASIC	FAU_SAA.1, FAU_SAA.4
O.DETECT_NETWORK_BASIC	ENV_IDS.1
O.DETECT_SITE_BASIC	ENV_IDS.1
O.ENTRY_NON_TECHNICAL	ENV_NON.1
O.ENTRY_Non_TOE	ENV_NON.1
O.ENTRY_TOE	FIA_UAU.1, FIA_UAU.7, FIA_UID.1
O.FORENSICS_PROC	ENV_FOR.1
O.HARDWARE_EXAM_MINIMUM	ENV_EXM.1
O.ID_DISABLE	FIA_AFL.1, FMT_REV.1, ENV_ATH.1
O.ID_REMOVAL	FMT_REV.1, FMT_SMR.2, ENV_ATH.1
O.ID_REVALIDATION	ENV_ATH.1
O.INFO_FLOW	FDP_ACC.2, FDP_IFC.1, FDP_IFF.1, ENV_INT.1
O.INTEGRITY_LOW	FDP_ACF.1
O.MALICIOUS_CODE	FAU_ARP.1
O.MANAGE_TOE	FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, FMT_SMR.2
O.MARK_COMPONENT	ENV_MRK.1
O.MARK_OUTPUT	ENV_MRK.1
O.MEDIA_REVIEW	ENV_MRK.1, ENV_REV.1
O.NETWORK_INTERFACE	ENV_INT.1
O.NTK_NNSA	FDP_ACC.2, FMT_MTD.1, FMT_REV.1, FPT_TST.1, FMT_SMR.2
O.PHY_MANDATED	ENV_PHY.1
O.PHYSICAL	ENV_PHY.1
O.PHYSICAL_PROTECTION	ENV_PHY.1
O.RECOVERY_CONTROLLED	FPT_RCV.1, AGD_ADM.1, ADV_SPM.1, ENV_RCV.1

O.RESIDUAL_PROTECTION	FDP_RIP.1
O.RESOURCE_USAGE	FRU_RSA.1
O.ROLES_OTHER_SECURITY	FMT_SMR.2, ENV_ROL.1
O.SEC_FUNC_MANAGEMENT	FIA_ATD.1, FIA_USB.1, FMT_MOF.1; FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMR.2, FMT_REV.1, FPT_AMT.1, FPT_TST.1
O.SESSION_ESTABLISHMENT	FIA_AFL.1, FIA_UAU.1, FIA_UID.1, FPT_TST.1, FTA_MCS.1, FTA_TSE.1
O.SOFTWARE_EXAM_MINIMUM	ENV_EXM.1
O.TRAINING	ENV_TNG.1
O.TRANS_SEC_UNCLASS	FCS_COP.1, FDP_ITC.1, FCS_CKM.4, FMT_MSA.2, ENV_PRO.1
O.TRUSTED_PATH	FTP_TRP.1
O.TSF_DOMAIN_SEPARATION	FPT_AMT.1, FPT_RVM.1, FPT_SEP.2
O.UNESCORT_ACCESS_UNCLASS	ENV_PHY.1
O.USER_INACTIVITY	FTA_SSL.1
O.USER_LOCKING	FTA_SSL.2
O.WARNING_BANNER	FTA_TAB.1, ENV_NOT.1