DRAFT

CS2 - Protection Profile Guidance for Near-Term COTS

DRAFT VERSION 0.5

by Gary Stoneburner (NIST)

Date - March 25, 1999

Revision History

Version 0.5, Date-TBD, Protection Profile Guidance
By Gary Stoneburner (NIST)
Incorporate lessons learned from development of OS profile

Version 0.4, December 10, 1998, Protection Profile Guidance
By Gary Stoneburner (NIST)
Revision of version 0.3, adding SOF; separated threats and objectives into environment, TOE, and joint TOE/Environment; and providing information on how to use guidance in producing a “compliant”PP.

Version 0.3, July 13, 1998, Protection Profile Guidance
By Gary Stoneburner (NIST)
Revision of version 0.2, updated to CC version 2 (May 98), reflecting requirements of mutual recognition agreements (MRA), and changing from PP to PP guidance. Modifications to lists of assumptions, threats, and objectives, and to the contents of CS2-EAL are scheduled for next version.

Version 0.2, March 6, 1998, Protection Profile
By Gary Stoneburner (NIST)
Major rework of version 0.1, focusing on near-term achievability and updating to CC version 2 (Dec 98).

Version 0.1, May 23 1997, Protection Profile
By Kristina C. Rogers (Cygnacom Solutions), built to CC version 1.0. Initial version, prepared for NIST under Contract Number 50SBNB6C9287/0353-96-6308

DRAFT

TABLE OF CONTENTS

SECTION **PAGE**

TABLE OF TABLES

SECTION PAGE

INTRODUCTION

1 Identification

Title: CS2 –Guidance on PPs for Near-Term COTS

Assurance level: EAL2 –augmented (EAL-CS2)

Registration: <To be filled in upon registration>

Keywords: Protection Profile Guidance, COTS, general-purpose operating systems, applications, networked information systems, baseline protection

2 overview

Purpose

The purpose of CS2 is to provide the guidance necessary to develop "compliant"protection profiles for near-term achievable, security baselines using commercial off the shelf (COTS) information technology.

CS2 accomplishes this purpose by:

- describing a largely policy-neutral, notional information system in the format of a protection profile (PP).

- specifying a subset of the common criteria to be used in developing “compliant”protection profiles
- providing the basis for refining -
- policy neutral guidance into specific policy requirements and
- system security threats, objectives, and requirements into a subset which is appropriate for a specific PP.

Scope

Type of system. CS2 provides the requirements necessary to specify needs for both stand-alone and distributed, multi-user information systems. This covers general-purpose operating systems, database management systems, and other applications.

Type of access. CS2 recognizes two forms of legitimate access; namely, public access and “authenticated users”. With public access, the user does not have a unique identifier and is not authenticated prior to access. An example is access to information on a publicly accessible web page. Such users have legitimate access, but are differentiated from “authenticated users”who are (1) uniquely identifiable by the system, (2) have legitimate access beyond publicly available information, and (3) are authenticated prior to being granted such access.

Nature of use. CS2 “compliant”PPs are suitable for the protection of information in real-world environments, both commercial and government.

- Within government environments, CS2 “compliant”PPs are considered to be suitable for specifying the baseline protection requirements for sensitive-but-unclassified or single level classified information in an environment where all authenticated users are cleared for the level of information being processed. For classified environments, public access is not allowed into CS2 “compliant”systems. For sensitive-but unclassified environments, public access may be acceptable with additional controls, beyond target of evaluation (TOE) supplied mechanisms, supplied by the operational environment.

- For commercial environments, CS2 “compliant”PPs are suitable for specifying the baseline protection requirements for information in environments where all authenticated users are either (1) trusted to not maliciously attempt to circumvent nor by-pass access controls or (2) lack the motivation or capability for sophisticated penetration attempts. Public access is allowed with environmental controls over and beyond the TOE supplied security mechanisms.

Key Assumptions. Key ~~environmental constraints~~ assumptions that apply for CS2 “compliant”PPs are –

- the TOE is comprised of near-term, commercial off the shelf (COTS) information technology
- authenticated users recognize the need for a secure IT environment
- authenticated users can be reasonably trusted to correctly apply the organization’s security policies in their discretionary actions

- ~~βασιχ πηψσιχαλ σεχυριτψ ισ προωιδεδ~~
- competent security administration is performed
- business/mission process automation is implemented with due regard for what CS2 "compliant"PPs do not expect of their TOEs.

Summary of CS2 Requirements

Assurance. CS2 assurances have been selected to provide the level of confidence resulting from (1) existing best practices for COTS development and (2) no extensive (and hence costly) third-party evaluation. This equates, in summary, to TOE technical countermeasures that -

- are sufficient for controlling a community of benign (i.e., not ~~intentionally~~ malicious) authenticated users
- ~~can~~ provide protection against unsophisticated, technical attacks
- ~~are~~ can not be expected to ~~protect~~ adequately protect against sophisticated, technical attacks (to include denial-of-service ~~attacks~~)

Functionality. The notional CS2 system targets these user needs -

- enforcing an access control policy between active entities (subjects) and passive objects based on subject identity, allowed actions, and environmental constraints such as time-of-day and port-of-entry
- enforcing information flow control policies at the macro (e.g., domain to domain) level
- resistance to resource depletion by providing resource allocation features
- providing mechanisms to detect some insecurities
- providing mechanisms for trusted recovery in the event of some system failures or detected insecurities
- supporting these capabilities in a distributed system connected via an untrusted network

CS2 "compliant"PPs are not expected to require that the TOE –

- provide the label-based controls appropriate for protecting controlled information (such as government classified, company proprietary, or export restricted data) in environments containing authenticated users who are not allowed access to such information
- adequately protect against malicious abuse of authorized privileges
- adequately protect against sophisticated attacks (to include denial of service)
- provide sufficient protection against installation, operation, or administration errors

1.

TOE DESCRIPTION

The Target of Evaluation (TOE) in a common criteria protection profile is the information technology component or system for which requirements are to be specified. This section, TOE Description, describes the CS2 class of protection profiles (PPs) in terms of the TOEs covered. These TOEs are identified by class of products, the operational environment, and the required security functionality.

1.1 Product class

CS2 provides PP guidance for PPs which include general-purpose operating systems and applications in both stand-alone and networked environments. The TOEs covered by such PPs permit one or more processors and attached peripheral and storage devices to be used by multiple users to perform a variety of functions requiring controlled, shared access to processing capability and information.

The TOE may be (1) a stand-alone system, (2) a distributed system, or (3) confined to a single host but intended to interface with a networked environment. The TOE will provide user services directly or serve as a platform for compliant applications. Unless explicitly stand-alone, the TOE will support protected communications across an untrusted network; unless of course, the network is a part of the TOE.

1.2 OPerational Environment

The TOE supports the active entities of human users and software processes. Human users, in conjunction with system processes, are accountable for all system activities. The TOE generates processes that act on behalf of either a specific human user or a uniquely identifiable system process. A process requests and consumes resources on behalf of its unique, associated user or system process. In a networked environment, a process may invoke another process on a different system.

A distributed TOE, or a TOE intended for use in a networked environment, will support one or more types of communication and protocols, such as:

- Synchronous process communication; e.g., remote procedure calls (RPC)
- Asynchronous process communication; e.g., message passing using user datagram protocol (UDP)
- Electronic mail; e.g., simple mail transfer protocol (SMTP)
- Dedicated network services; e.g., hypertext transfer protocol (HTTP)
- Network management protocols; e.g., simple network management protocol (SNMP)

A compliant TOE will generally support –

- Users with networked access to the TOE across an untrusted network (that is, mechanisms operating within the TOE cooperate with mechanisms in other components to securely exchange information across an untrusted network)

- Several users executing tasks on the same system concurrently
- Sharing resources, such as printer and mass storage, across a network

1.1 required security functionality

CS2 specifies the requirements for a system with the security functionality listed below. A specific CS2 "compliant" PP will call out that subset of this functionality which is appropriate for the specific environment and type of TOE it covers.

- Executing the access control policy of the imposed IT security policy
- Assigning a unique identifier to each authenticated user
- Assigning a unique identifier to each system process, including those not running on behalf of a human user (e.g., processes started at system bootup like the Unix "inetd")
- Authenticating the claimed user identity before allowing any user to perform any actions other than a well-defined set of operations (e.g., reading from a public web site)
- Auditing in support of individual accountability and detection of and response to insecurity
- Enabling access authorization management; i.e., the initialization, assignment, and modification of access rights (e.g. read, write, execute) to data objects with respect to (1) active entity name or group membership and (2) environmental constraints such as time-of-day and port-of-entry.
- Resource allocation features providing a measure of resistance to resource depletion
- Mechanisms for detecting some insecurities
- System recovery features providing a measure of survivability in the face of system failures and insecurities
- Automated support to help in the verification of secure delivery, installation, operation, and administration

2.

Security environment

~~{Editorial note: Work is still required to produce assumptions and threats with broad consensus.}~~

2.1 INTRODUCTION

This section identifies the following:

- significant assumptions about the TOE and its operational environment for CS2 “compliant”PPs
- organizational security policies for which CS2 compliant PPs are appropriate
- IT-related threats to the organization countered by the information technology in the notional CS2 information system
- threats requiring reliance on environmental controls to provide sufficient protection
- general description of the assurance required for CS2

By providing the information describe above, this section gives the basis for the security objectives described in section 4 and hence the specific security requirements listed in sections 5 and 6.

2.1

Secure Usage Assumptions

The specific conditions listed below are assumed to exist in a CS2 environment. These assumptions include both practical realities to be considered in the development of security requirements in CS2 "compliant"PPs and essential environmental constraints on the use of TOEs compliant with such a PP.

Table 3.2-1 –Security assumptions - TOE

Name	Assumption	Discussion
A.COTS	The TOE is constructed from near-term achievable, commercial off the shelf information technology.	This assumption is a key driver in determining the nature of the expectations toward, and hence the requirements to placed upon, the TOE.
A.MALICIOUS-INSIDER	The TOE is not expected to be able to sufficiently mitigate the risks resulting from malicious abuse of authorized privileges.	It is not reasonable to expect near-term COTS products to provide sufficient protection against the malicious actions of authorized individuals.
A.NO-LABELS	The TOE does not have to provide label-based access controls.	It is an assumption, based upon currently available technology and current common practice, that label based access controls will not be included in near-term COTS.
A.SOPHISTICATED-ATTACK	The TOE is not expected to be able to sufficiently mitigate risks resulting from application of sophisticated attack methods.	It is not reasonable to expect near-term achievable COTS to be able to resist sophisticated attacks.

Table 3.2-2 – Security assumptions - Personnel

Name	Assumption	Discussion
~~A.PHYSICAL~~	~~The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.~~	~~A TOE will not be able to meet its security requirements unless at least a minimum degree of physical security is provided.~~
A. ADMIN	The security features of the TOE are competently administered on an on-going basis.	It is essential that security administration be both competent and on-going.
A.USER-NEED	Authenticated users recognize the need for a secure IT environment.	It is essential that the authenticated users appreciate the need for security. Otherwise they are likely to try and circumvent it.
A.USER-TRUST	Authenticated users are generally trusted to perform discretionary actions in accordance with security policies.	Authenticated users will have a fair amount of discretion with CS2 systems. It is important that they be adequately trained and motivated to make wise choices in these actions. This "trust"is not absolute, but must be a reasonable expectation. Hence the phrase "generally trusted"

ORGANIZATIONAL security policies

The organizational security policies discussed below are addressed by the notional CS2 information system.

Table 3.3-1 –Security policies

Name	Policy	Discussion
P.ACCESS	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.	CS2 supports organizational policies which grant or deny access to objects using rules driven by attributes of the user (such as user identity, group, etc.), attributes of the object (such as permission bits), type of access (such as read or write), and environmental conditions (such as time-of-day).
P.ACCOUNT	Users must be held accountable for security-relevant actions.	CS2 supports organizational policies requiring that users are held accountable for their actions, facilitating after-the-fact investigations and providing some deterrence to improper actions.
P.COMPLY	The implementation and use of the organization's IT systems must comply with all applicable laws, regulations, and contractual agreements imposed on the organization.	The organization will meet all requirements imposed upon it from the outside; for example: government regulations, national and local laws, and contractual agreements.
P.DUE-CARE	The organization's IT systems must be implemented and operated in a manner that represents due care and diligence with respect to risks to the organization.	It is important that the level of security afforded the IT system be in accordance with what is generally considered adequate within the business or government sector in which the organization is placed.
P.INFO-FLOW	Information flow between IT components must be in accordance with established information flow policies.	CS2 includes information flow control as this is needed in many environments. Whether this is a part of a specific PP depends upon the policy that PP is intending to cover.
P.KNOWN	Except for a well-defined set of allowed operations, users of the TOE must be identified and authenticated before TOE access can be granted.	Beyond a well-defined set of actions such as read access to a public web-server, there is a finite community of known, authenticated users who are authenticated before being allowed access.
P.NETWORK	The organization's IT security policy must be maintained in the environment of distributed systems interconnected via insecure networking.	Since CS2 systems will likely be interconnected across untrusted networking, this policy statement will have a significant impact on CS2 requirement definition.
P.PHYSICAL	The processing resources of the TOE that must be physically protected in order to ensure that security objectives are met, will be located within controlled access facilities that mitigate unauthorized, physical access.	A TOE will not be able to meet its security requirements unless at least a minimum degree of physical security is provided.
P.SURVIVE	The IT system, in conjunction with its environment, must be resilient to	CS2 systems will provide a measure of this resilience through functionality and assurances that resist,

	insecurity, resisting the insecurity and/ or providing the means to detect an insecurity and recover from it.	detect, and recover from insecurities. For sophisticated attacks, a large portion of this resilience is provided by the TOE environment.
P.TRAINING	Authenticated users of the system must be adequately trained, enabling them to (1) effectively implement organizational security policies with respect to their discretionary actions and (2) support the need for non-discretionary controls implemented to enforce these policies.	Once granted legitimate access, authenticated users are expected to use IT resources and information only in accordance with the organizational security policy. In order for this to be possible, these users must be adequately trained both to understand the purpose and need for security controls and to be able to make secure decisions with respect to their discretionary actions.
P.USAGE	The organization's IT resources must be used for only for authorized purposes.	CS2 systems must, in conjunction with its environment, ensure that the organization's information technology is not used for unauthorized purposes.

2.2

Threats to security

The technical countermeasures of the notional CS2 system are required to counter threats which may be broadly categorized as -

- the threat of unsophisticated, malicious attacks from individuals other than authenticated users
- the threat of authenticated users attempting, non-maliciously to gain unauthorized access or to perform an unauthorized operation. Such attempts may be performed to "get the job done", out of curiosity, as a challenge, or as a result of an error.

Other threats that can affect system security must be dealt with in conjunction with controls provided by the operating environment.

The threats facing CS2 systems are listed in Tables 3.4-1 through 3.4-3 and discussed further in sections 3.4.1 through 3.4.3 as follows:

Table 3.4-1 and section 3.4.1: Threats addressed by the environment

Table 3.4-2 and section 3.4.2: Threats addressed by the TOE

Table 3.4-3 and section 3.4.3: Threats addressed jointly by the TOE and its environment

Threats addressed by the TOE's environment

The purpose of this section is to identify those threats that are important for the intended audience of the PP. Additionally, threats are listed to sufficiently identify what must be addressed by the TOE's environment. This is done to facilitate the composition of a CS2 compatible system with the TOE of a given PP. Some of the threats in Table 3.4-1 are expected in every CS2 "compliant"PP; for example T.DENIAL-SOPHISTICATED which is beyond the assurances expected from near-term COTS. Other threats may not be needed, as the TOE fully covers them; for example, if the TOE is the underlying operating system then T.RESOURCES-Non-TOE may be unnecessary as an environmental threat and T.RESOURCES-TOE might be relabeled as T.RESOURCES for that PP.~~It is expected that all CS2 "compliant" PPs will include the threats listed in Table 3.4-1. In addition, since a specific PP narrows the scope to a specific IT product within the system, that PP will likely add to this list threats from Tables 3.4-2 and 3.4-3. These added threats represent what will be satisfied by the IT, other than the TOE, in the notional CS2 system. (In the CS2 "compliant" PP, sections 3.4.1 through 3.4.3 will be adjusted to correspond to these changes in Tables 3.4-1 through 3.4-3. Additionally, these changes must be reflected in Section 4 "Security Objectives"of the "compliant" PP.)~~

Table 3.4-1 –Security threats addressed by TOE's Environment

T.ACCESS-NON-TECHNICAL	An authenticated user may gain non-malicious, unauthorized access using non-technical means.
T.ACCESS-Non-TOE	An authenticated user may gain unauthorized, non-malicious access to a resource or to information not directly controlled by the TOE via user error, system error, or an unsophisticated, technical attack.
T.AUDIT-CONFIDENTIALITY-Non-TOE	For audit trails not under control of the TOE, records of security events may be disclosed to unauthorized individuals or processes.
T.AUDIT-CORRUPTED-Non-TOE	For audit trails not under control of the TOE, records of security events may be subjected to unauthorized modification or destruction.
T.DENIAL-Non-TOE	The IT (other than the TOE) may be subjected to an unsophisticated, denial-of-service attack.
T.DENIAL-SOPHISTICATED	The system may be subjected to a sophisticated, denial-of-service attack.
T.ENTRY-NON-TECHNICAL	An individual, other than an authenticated user, may gain access to processing resources or information using non-technical means.
T.ENTRY-Non-TOE	An individual other than an authenticated user may gain unauthorized, malicious access to processing resources or information not controlled by the TOE via an unsophisticated, technical attack.
T.ENTRY-SOPHISTICATED	An individual, other than an authenticated user, may gain access to processing resources or information using a sophisticated, technical attack.
T.OBSERVE-Non-TOE	Events occur in operation of IT (other than the TOE) that compromise IT security; but that IT, due to flaws in its specification, design, or implementation, may lead a competent user or security administrator to believe that the system is still secure.
T.PHYSICAL	Security-critical parts of the ~~TOE~~ system may be subjected to a physical attack that may compromise security.
T.RECORD-EVENT-Non-TOE	Security relevant events not under control of the TOE may not be recorded.
T.RESOURCES-Non-TOE	The shared, internal resources of IT other than the TOE may become exhausted due to system error or non-malicious user actions.
T.TRACEABLE-Non-TOE	Security relevant events not under control of the TOE may not be traceable to the user or system process associated with the event.

Threats addressed by the TOE

~~While all of the threats listed in Table 3.4-2 will appear in a~~A CS2 “compliant”PP~~, that PP~~ will tailor ~~these~~ the threats listed in Table 3.4-2 to the specifics of the operational environment being addressed and the nature of the TOE within that environment. This is done by eliminating threats that do not apply (e.g., T.RESOURCES-TOE for a TOE that does not manage shared resources) or by moving threats that are not addressed by that TOE into Table 3.4-1 (threats addressed by the environment) and moving threats addressed jointly by that TOE and the remaining IT in the notional CS2 system into Table 3.4-3 (jointly addressed threats). (In the CS2 “compliant”PP, sections 3.4.1 through 3.4.3 will be adjusted to correspond to these changes to Tables 3.4-1 through 3.4-3. Additionally, these changes must be reflected in Section 4 “Security Objectives”of the “compliant”PP.)

Table 3.4-2 –Security threats addressed by TOE

Name	**Threat**
T.ACCESS-TOE	An authenticated user may gain unauthorized, non-malicious access to the TOE, or a resource or to information directly controlled by the TOE via user error, system error, or an unsophisticated, technical attack.
T.AUDIT-CONFIDENTIALITY-TOE	~~Records~~ For audit trails under control of the TOE, records of security events may be disclosed to unauthorized individuals or processes.
T.AUDIT-CORRUPTED-TOE	~~Records~~ For audit trails under control of the TOE, records of security events may be subjected to unauthorized modification or destruction.
T.CRASH-TOE	The secure state of the TOE could be compromised in the event of a system crash.
T.DENIAL-TOE	The TOE may be subjected to an unsophisticated, denial-of-service attack.
T.ENTRY-TOE	An individual other than an authenticated user may gain unauthorized, malicious access to TOE controlled processing resources or information via an unsophisticated, technical attack.
T.OBSERVE-TOE	Events occur in TOE operation that compromise IT security but the TOE , due to flaws in its specification, design, or implementation, may lead a competent user or security administrator to believe that the system is still secure.
T.RECORD-EVENT-TOE	Security relevant events controlled by the TOE may not be recorded.
T.RESOURCES-TOE	The shared, internal TOE resources may become exhausted due to system error or non-malicious user actions.
T.TOE-CORRUPTED	The security state of the TOE, as a result of a lower-grade attack, may be intentionally corrupted to enable future insecurities.
T.TRACEABLE-TOE	Security relevant events controlled by the TOE may not be traceable to the user or system process associated with the event.

Threats addressed jointly by the TOE and its environment

In a specific CS2 “compliant”PP, the TOE (as a subset of the overall, notional CS2 system) may not be able to help address some of the threats listed in Table 3.4-3. In that case such threats would be moved into Table 3.4-1 (threats addressed by the environment) for that PP. It is also possible that PP author may decide to specify the nature of compliant solutions more stringently than this CS2 PP guidance has done. It that case some of the jointly addressed threats may become either a TOE addressed threat and be moved into Table 3.4-2 or an environmental addressed threat and be moved into Table 3.4-1. (In the CS2 “compliant” PP, sections 3.4.1 through 3.4.3 will be adjusted to correspond to these changes to Tables 3.4-1 through 3.4-3. Additionally, these changes must be reflected in Section 4 “Security Objectives”of the “compliant” PP.)

Table 3.4-3 –Security threats addressed Jointly by TOE and Environment

T.ACCESS-MALICIOUS	An authenticated user may obtain unauthorized access for malicious purposes.
T.ADMIN-ERROR	The security of the TOE may be reduced or defeated due to errors or omissions in the administration of the security features of the TOE.
T.CRASH-SYSTEM	The secure state of the system could be compromised in the event of a system crash.
T.INSTALL	The TOE may be delivered or installed in a manner that undermines security.
T.OPERATE	Security failures may occur because of improper operation of the TOE; e.g., the abuse of authorized privileges.
T.SYSTEM-CORRUPTED	The security state of the ~~TOE~~system, as a result of another threat, may be intentionally corrupted to enable future insecurities.

Threats environment addresses
The threats discussed below must be countered but are not addressed by the technical countermeasures within the notional CS2 system. Such threats must therefore, be addressed in conjunction with the operating environment.

T.ACCESS-NON-TECHNICAL: An authenticated user may gain non-malicious, unauthorized access using non-technical means.

The use of non-technical attack means; for example, social engineering or dumpster diving; is beyond the scope of TOE protections and must be addressed by the environment.

T.ACCESS-Non-TOE: An authenticated user may gain unauthorized, non-malicious access to a resource or to information not controlled by the TOE via user error, system error, or an unsophisticated, technical attack.

An authenticated user is someone who is (1) uniquely identifiable by the system, (2) has legitimate access beyond publicly available information, and (3) is authenticated prior to being granted such access.

By virtue of having access, the threat posed from authenticated users is inherently greater than that posed from unauthorized individuals. CS2 systems are expected to have only the assurances necessary to cover the threat of non-malicious actions by authenticated users; i.e., sufficient confidence in light of the fact that only non-malicious actions are covered.

There are two broad categories of users with respect to this threat:

- The first category are persons who possess little technical skills, do not have access to sophisticated attack tools, they have some rights of access, and are mostly trusted not to attempt to maliciously subvert the system nor maliciously exploit the information stored thereon. Users in this category may be motivated by curiosity to gain access to information for which they have no authorization.

- The second category of users is technically skilled or has access to sophisticated attack tools and some may attempt to bypass system controls as a technical challenge or as a result of curiosity. CS2 compliant components and systems would generally be used in environments where these users are highly trusted not to attempt to maliciously subvert the system nor to maliciously exploit the information stored thereon.

T.AUDIT-CONFIDENTIALITY-Non-TOE: Records of security events not under control of the TOE may be disclosed to unauthorized individuals or processes.

System security depends in part on the ability of the system to detect and report the occurrence of security relevant events, to determine the identity of those responsible for such events, and to protect the event records from unauthorized access, modification, or destruction.

T.AUDIT-CORRUPTED-Non-TOE: Records of security events not under control of the TOE may be subjected to unauthorized modification or destruction.

T.DENIAL-Non-TOE: The IT other than the TOE may be subjected to an unsophisticated, denial-of-service attack.

The IT in the TOE environment is expected to be able to withstand unsophisticated denial-of-service attacks.

T.DENIAL-SOPHISTICATED: The system may be subjected to a sophisticated, denial-of-service attack.

A system built from near-term COTS is not expected to be capable of resisting sophisticated attacks. Therefore, such a system must ~~The TOE is not capable of resisting sophisticated attacks and must therefore,~~ rely on protections provided by its environment to maintain availability in the face of such threats.

T.ENTRY-NON-TECHNICAL: An individual, other than an authenticated user, may gain access to processing resources or information using non-technical means.

T.ENTRY-Non-TOE: An individual other than an authenticated user may gain unauthorized, malicious access to processing resources or information not controlled by the TOE via an unsophisticated, technical attack.

The mechanisms and assurances of a near-term COTS system will resist low-grade technical attacks. (Resistance to higher-grade attacks, when such resistance is required, must be provide by the system's operational environment.)

T.ENTRY-SOPHISTICATED: An individual, other than an authenticated user, may gain access to processing resources or information using a sophisticated, technical attack.

A system built from near-term COTS is not expected to protect itself against sophisticated, technical attacks. Therefore, this threat is largely addressed by the system's operational environment.~~The TOE is not required to protect against sophisticated, technical attacks. There is no reasonable expectation that a TOE compliant with a CS2 PP will significantly increase, over that associated with a non-compliant TOE, the work-factor required to accomplish a successful, high-grade attack. Therefore, this threat is largely addressed by the TOE environment.~~

T.OBSERVE-Non-TOE: Events occur in operation of IT other than the TOE that compromise security but the IT, due to flaws in its specification, design, or implementation, may lead a competent user or security administrator to believe that the system is still secure.

This is the threat of an administrator or user not detecting a security problem because of errors or omissions in the IT's human interface. The IT is then used in a manner which is insecure but which the administrator or user reasonably, but incorrectly, believes to be secure.

T.PHYSICAL: Security-critical parts of the ~~TOE~~ system may be subjected to a physical attack that may compromise security.

The security offered by CS2 can be assured only to the extent that the hardware and software relied upon to enforce the security policy is physically protected from unauthorized physical modification

and from technical attacks at the hardware level. Examples of such attacks are using electromagnetic pulse weapons, intercepting radiated electronic emissions, and passive monitoring or active attacking of physical transmission medium (e.g., coax, twisted-pair, or fiber optic cable).

T.RECORD-EVENT-Non-TOE: Security relevant events which IT other than the TOE is expected to record may not be recorded.

T.RESOURCES-Non-TOE: The shared, internal resources of IT other than the TOE may become exhausted due to system error or non-malicious user actions.

System availability depends partly on the availability of shared resources.

T.TRACEABLE-Non-TOE: Due to the IT other than the TOE, security relevant events may not be traceable to the user or system process associated with the event.

2.2.1

Threats TOE addresses

Technical countermeasures within the notional CS2 system address the threats discussed below.

T.ACCESS-**TOE**: An authenticated user may gain unauthorized, non-malicious access to a resource or to information controlled by the TOE via user error, system error, or an unsophisticated, technical attack.

An authenticated user is someone who is (1) uniquely identifiable by the system, (2) has legitimate access beyond publicly available information, and (3) is authenticated prior to being granted such access.

By virtue of having access, the threat posed from authenticated users is inherently greater than that posed from unauthorized individuals. CS2 systems are required to have only the assurances necessary to cover the threat of non-malicious actions by authenticated users; i.e., sufficient confidence in light of the fact that only non-malicious actions are covered.

There are two broad categories of users with respect to this threat:

- The first category are persons who possess little technical skills, do not have access to sophisticated attack tools, and, because they have some rights of access, are mostly trusted not to attempt to maliciously subvert the system nor maliciously exploit the information stored thereon. Users in this category may be motivated by curiosity to gain access to information for which they have no authorization.

- The second category of users is technically skilled or has access to sophisticated attack tools and some may attempt to bypass system controls as a technical challenge or as a result of curiosity. CS2 compliant components and systems would generally be used in environments where these users are highly trusted not to attempt to maliciously subvert the system nor to maliciously exploit the information stored thereon.

T.AUDIT-CONFIDENTIALITY-**TOE**: Records of security events under control of the TOE may be disclosed to unauthorized individuals or processes.

TOE security depends in part on the ability of the TOE to detect and report the occurrence of security relevant events, to determine the identity of those responsible for such events, and to protect the event records from unauthorized access, modification, or destruction.

T.AUDIT-CORRUPTED-**TOE**: Records of security events under control of the TOE may be subjected to unauthorized modification or destruction.

T.CRASH-**TOE**: The secure state of the TOE could be compromised in the event of a system crash.

For the TOE to protect the information it controls, it must remain in a secure state, including after recovery from a system failure or discontinuity of service.

System crash can occur with inadequate mechanisms for secure recovery. ~~User d~~Data objects and audit information may be modified or lost and system or application software may be corrupted.

T.DENIAL-**TOE**: The TOE may be subjected to an unsophisticated, denial-of-service attack.

The ~~system~~ TOE must be able to withstand unsophisticated denial-of-service attacks.

T.ENTRY-**TOE**: An individual other than an authenticated user may gain unauthorized, malicious access to processing resources or information controlled by the TOE via an unsophisticated, technical attack.

The mechanisms and assurances of a TOE compliant with a CS2 PP will resist low-grade technical attacks. (Resistance to higher-grade attacks, when such resistance is required, must be provided in conjunction with ~~by~~ the TOE operational environment.)

T.OBSERVE-**TOE**: Events occur in TOE operation that compromise IT security but the TOE , due to flaws in its specification, design, or implementation, may lead a competent user or security administrator to believe that the system is still secure.

This is the threat of an administrator or user not detecting a security problem because of errors or omissions in the TOE's human interface. The TOE is then used in a manner which is insecure but which the administrator or user reasonably, but incorrectly, believes to be secure.

T.RECORD-EVENT-**TOE**: Security relevant events which the TOE is expected to record may not be recorded.

T.RESOURCES-**TOE**: The shared, internal TOE resources may become exhausted due to system error or non-malicious user actions.

System availability depends partly on the availability of shared resources.

T.TOE-CORRUPTED: The security state of the TOE, as a result of a lower-grade attack, may be intentionally corrupted to enable future insecurities.

System security depends to a large degree on the integrity of the hardware and software implementing the security functionality. If this is intentionally corrupted, the TOE will be unable to maintain a secure state.

T.TRACEABLE-**TOE**: ~~Security~~ Due to the TOE, security relevant events may not be traceable to the user or system process associated with the event.

2.2.1

Threats TOE and Environment jointly address

T.ACCESS-MALICIOUS: An authenticated user may obtain unauthorized access for malicious purposes.

CS2 functionality and assurances are sufficient mitigation for non-malicious actions by authenticated users. The greater risk from malicious actions by authenticated users must be addressed in conjunction with the environment.

T.ADMIN-ERROR: The security of the ~~TOE~~ system may be reduced or defeated due to errors or omissions in the administration of the security features of the TOE or other IT.

Authenticated users or external threat agents may, through accidental discovery or directed search, discover inadequacies in the security administration of the TOE, or other IT, which permit them to gain unauthorized access.

This threat is only partly covered by the TOE and therefore must also be addressed by the TOE environment.

T.CRASH-SYSTEM: The secure state of the system could be compromised in the event of a system crash.

For the IT to protect the information it controls, it must remain in a secure state, including after recovery from a system failure or discontinuity of service. System crash can occur with inadequate mechanisms for secure recovery. User data objects and audit information may be modified or lost and system or application software may be corrupted.

The TOE is unable to, in general, ensure recovery for IT other than itself. However, depending upon the specifics of a given TOE, it may well help support the recovery of other IT in its environment.

T.INSTALL: The ~~TOE~~ system may be delivered or installed in a manner that undermines security.

The security offered by CS2 is predicated upon the ~~TOE~~ IT being initially established in a secure state. That includes assurance that the TOE delivered is that which was evaluated and that the TOE, and other IT, is subsequently installed properly. While the TOE is expected to provide mechanisms to support mitigating against this threat, the support of the environment is critical.

T.OPERATE: Security failures may occur because of improper operation of the TOE; e.g., the abuse of authorized privileges.

The security offered by CS2 can be assured only to the extent that the TOE, and other IT, is operated correctly by system administrators and authenticated users in accordance with security policy. The TOE will provide mechanisms that help mitigate this threat. Yet specific environmental controls are also required.

T.SYSTEM-CORRUPTED: The security state of the system, as a result of corruption of IT other than the TOE or as a result of a higher-grade attack, may be intentionally corrupted to enable future

insecurities. ~~The security state of the TOE, as a result of another threat, may be intentionally corrupted to enable future insecurities.~~

System security depends to a large degree on the integrity of the hardware and software implementing the security functionality. If this is intentionally corrupted, the IT will be unable to maintain a secure state. Cooperation between the TOE and its environment is required because (1) the TOE can only partially protect against higher-grade threats and (2) the TOE may be a necessary part of protecting IT other than the TOE from lower-grade attacks. (See T.TOE-CORRPUTED for corruption of the TOE by lower-grade attacks.) ~~The TOE security depends to a large degree on the integrity of the hardware and software implementing the security functionality. If this is intentionally corrupted, the TOE will be unable to maintain a secure state. The TOE can only partially protect against this threat.~~

2.3

General assurance need

CS2 “compliant”PPs are targeted for near-term achievable, cost-effective, COTS security. In keeping with this target, the general level of assurance for CS2 must:

- be consistent with current best commercial practice for IT development and
- enable evaluated products that are competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

CS2 assurance must also, to enhance wide-spread acceptance, be consistent with current and near-term mutual recognition arrangement. This requires that the CS2 assurances:

- be expressed as an existing evaluation assurance level (EAL) from part 3 of the Common Criteria; augmented by CC assurance components as required
- contain no assurance components first appearing in EAL5 or above

In keeping with these requirements, the general level of assurance needed for CS2 is EAL2 augmented to include other vendor actions within the scope of current best commercial practice.

3.

security objectives

~~(Editorial note: Work is still required to produce objectives with broad consensus.)~~

3.1 Environmental security objectives

Addressing some policies and threats is beyond the capabilities of the notional CS2 system. These result in the objectives listed in Table 4-1. The CS2 system does not contribute significantly to meeting these objectives.

~~It is expected that all CS2 "compliant"PPs will list these environmental objectives.~~The purpose of the environmental objectives (in conjunction with the Joint objectives) is to state what is expected of the TOE's environment. This is done primarily to facilitate determining the security requirements which the environment must meet in order to compose a CS2 "compliant"system using the TOE of a given PP. ~~In addition, s~~Since a specific PP narrows the scope to a specific IT product within the system, that PP ~~will likely~~ may add to this list objectives from Tables 4.2 and 4.3. These added objectives represent what will be satisfied by the IT, other than the TOE, in the notional CS2 system. Additionally, for a specific TOE, some of the objectives in Table 4.1 may be eliminated as unnecessary; for example, if the TOE is the underlying operating system then O.RESOURCES-Non-TOE may be unnecessary as an environmental objective and O.RESOURCES-TOE might be relabeled as O.RESOURCES for that PP. (These changes must be consistent with the threat categorizations in section 3.4 "Threats to Security"of the "compliant"PP.)

Table 4-1 –Environmental Security Objectives

Environmental Security Objective	Corresponding Threat or Policy
~~O.ACCESS-MALICIOUS: The TOE environment must sufficiently mitigate the threat of malicious actions by authenticated users.~~	~~T.ACCESS-MALICIOUS~~
O.ACCESS-NON-TECHNICAL: The TOE environment must provide sufficient protection against non-technical attacks by authenticated users for non-malicious purposes. This will be accomplished primarily via prevention with a goal of high effectiveness. Personnel security and user training and awareness will provide a major part of achieving this objective.	T.ACCESS-NON-TECHNICAL
O.ACCESS-Non-TOE: The IT other than the TOE must provide public access and access by authenticated users to the resources and actions for which they have been authorized and over which the TOE does not exercise control. This is expected with a high degree of effectiveness.	P.ACCESS
O.ACCOUNT-Non-TOE: The IT other than the TOE must ensure, for actions under its control or knowledge, that all users can subsequently be held accountable for their security relevant actions. This is expected with a high degree of effectiveness.	P.ACCOUNT T.TRACEABLE-Non-TOE T.RECORD-EVENT-Non-TOE T.AUDIT-CORRUPTED-Non-TOE T.AUDIT-CONFIDENTIALITY-Non-TOE
O.AUTHORIZE-Non-TOE: The IT other than the TOE must provide the ability to specify and manage user and system process	P.ACCESS

access rights to individual processing resources and data elements under its control, supporting the organization's security policy for access control. This is expected with a high degree of effectiveness. NOTE: This includes initializing, specifying and managing (1) object security attributes, (2) active entity identity and security attributes, and (3) security relevant environmental conditions.	
O.AVAILABLE-Non-TOE: The IT other than the TOE must protect itself from unsophisticated, denial-of-service attacks. This is a combination of prevention and detect and recover with a high degree of effectiveness.	P.SURVIVE T.DENIAL-Non-TOE
O.BYPASS-Non-TOE: For access not controlled by the TOE, IT other than the TOE must prevent errant or non-malicious, authorized software or users from bypassing or circumventing security policy enforcement. This will be accomplished with high effectiveness. NOTE: This objective is limited to 'non-malicious'because IT controls in the notional CS2 system are not expected to provide sufficient mitigation for the greater negative impact that 'malicious'implies.	T.ACCESS-Non-TOE
O.DENIAL-SOPHISTICATED: The TOE environment must maintain system availability in the face of sophisticated denial-of-service attacks. The focus is on detection and response with a goal of moderate effectiveness.	P.SURVIVE T.DENIAL-SOPHISTICATED
O.DETECT-SOPHISTICATED: The TOE environment must provide the ability to detect sophisticated attacks and the results of such attacks (e.g., corrupted system state). The goal is for moderate effectiveness.	P.SURVIVE T.SYSTEM-CORRUPTED
O.ENTRY-NON-TECHNICAL: The TOE environment must provide sufficient protection against non-technical attacks by other than authenticated users. This will be accomplished primarily via prevention with a goal of high effectiveness. User training and awareness will provide a major part of achieving this objective.	T.ENTRY-NON-TECHNICAL
O.ENTRY-Non-TOE: For resources not controlled by the TOE, IT other than the TOE must prevent logical entry using unsophisticated, technical methods, by persons without authority for such access. This is clearly a prevent focus and is to be achieved with a high degree of effectiveness.	P.USAGE T.ENTRY-Non-TOE
O.ENTRY-SOPHISTICATED: The TOE environment must sufficiently mitigate the threat of an individual (other than an authenticated user) gaining unauthorized access via sophisticated, technical attack. This will be accomplished by focusing on detection and response with a goal of moderate effectiveness.	T.ENTRY-SOPHISTICATED
O.KNOWN-Non-TOE: The IT other than the TOE must ensure that, for all actions under its control and except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access. This is expected with a high degree of effectiveness.	P.KNOWN
O.OBSERVE-Non-TOE: The IT other than the TOE must ensure that its security status is not misrepresented to the administrator or user. This is a combination of prevent and detect and, considering the potentially large number of possible failure modes, is to be achieved with a moderate, verses high, degree of effectiveness.	T.OBSERVE-Non-TOE

O.PHYSICAL: Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security.	T.PHYSICAL P.PHYSICAL
O.RESOURCES-Non-TOE: IT other than the TOE must protect itself from user or system errors that result in shared resource exhaustion. This will be accomplished via protection with high effectiveness.	P.SURVIVE T.RESOURCES-Non-TOE

TOE security objectives

While the environment contributes to the satisfaction of nearly all objectives, those listed here are satisfied by the TOE with only generic environmental support such as user training.

Table 4-1 gives the security objectives to be met by the notional CS2 information system.

While all of the TOE objectives will ~~appear~~ be covered in a CS2 "compliant" PP, that PP will tailor these objectives to the specifics of the operational environment being addressed and the nature of the TOE within that environment. This is done by eliminating objectives that do not apply (for example, if the TOE does not manage shared resources, then O.RESOURCES-TOE does not apply), moving objectives that are not addressed by that TOE into Table 4-1 (environmental objectives) and moving objectives addressed jointly by that TOE and the remaining IT in the notional CS2 system into Table 4-3 (joint objectives). (These changes must be consistent with the threat categorizations in section 3.4 "Threats to Security"of the "compliant"PP.)

Table 4-2 –TOE Security Objectives

IT Security Objective	Corresponding Threat or Policy
O.ACCESS-TOE: The TOE must provide public access and access by authenticated users to those TOE resources and actions for which they have been authorized. This will be accomplished with high effectiveness.	P.ACCESS
O.ACCOUNT-TOE: The TOE must ensure, for all actions under its control or knowledge, that all TOE users can subsequently be held accountable for their security relevant actions. This will be done with moderate effectiveness, in that it is anticipated that individual accountability might not be achieved for some actions.	P.ACCOUNT T.TRACEABLE-TOE T.RECORD-EVENT-TOE T.AUDIT-CORRUPTED-TOE T.AUDIT-CONFIDENTIALITY-TOE
O.AUTHORIZE-TOE: The TOE 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. This will be accomplished with high effectiveness. NOTE: This includes initializing, specifying and managing (1) object security attributes, (2) active entity identity and security attributes, and (3) security relevant environmental conditions.	P.ACCESS
O.AVAILABLE-TOE: The TOE must protect itself from unsophisticated, denial-of-service attacks. This will include a combination of protection and detection with high effectiveness.	P.SURVIVE T.DENIAL-TOE
O.BYPASS-TOE: The TOE must prevent errant or non-malicious,	T.ACCESS-TOE

authorized software or users from bypassing or circumventing TOE security policy enforcement. This will be accomplished with high effectiveness. NOTE: This objective is limited to 'non-malicious'because CS2 controls are not expected to be sufficient mitigation for the greater negative impact that 'malicious'implies.	
O.DETECT-TOE: The TOE must enable the detection of insecurities. The goal is high effectiveness for lower grade attacks. Note: The level of detection provided by the TOE is only that corresponding to the level of attack sophistication being protected against by the other IT-objectives.	P.SURVIVE T.~~SYSTEM~~TOE-CORRUPTED
O.ENTRY-TOE: The TOE must prevent logical entry to the TOE using unsophisticated, technical methods, by persons without authority for such access. This will be accomplished with high effectiveness.	P.USAGE T.ENTRY-TOE
~~O.INFO-FLOW: The TOE must ensure that any information flow control policies are enforced - (1) between TOE components and (2) at the TOE external interfaces.~~	~~P.INFO-FLOW~~
O.KNOWN-TOE: The TOE must ensure that, for all actions under its control and except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access. This will be accomplished with high effectiveness.	P.KNOWN
~~O.NETWORK: Unless explicitly stand-alone, the TOE must be able to meet its security objectives in a distributed environment. This may be either as a distributed TOE and as a TOE networked with other IT resources.~~	~~P.NETWORK~~
O.OBSERVE-TOE: The TOE must ensure that its security status is not misrepresented to the administrator or user. This is a combination of prevent and detect and, considering the potentially large number of possible failure modes, is to be achieved with a moderate, verses high, degree of effectiveness.	T.OBSERVE-TOE
O.RECOVER-TOE: The TOE must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecurity. This will be accomplished with a high effectiveness for specified failures and a low effectiveness for failures in general.	P.SURVIVE T.CRASH-TOE
O.RESOURCES-TOE: The TOE must protect itself from user or system errors that result in shared resource exhaustion. This will be accomplished via protection with high effectiveness.	P.SURVIVE T.RESOURCES-TOE

3.2

Joint TOE/Environment security objectives

The objectives listed here fall into one or more of the following categories:

a. The TOE and its environment together satisfy the objective as follows:

1) TOE - contributes in a significant manner and

2) Environment - contribution is specific to this objective; i.e, not the result of a general contribution such as user training.

b. At the level of abstraction of the PP either:

1) It is not possible to accurately determine the split between TOE and environmental contribution, or

2) Multiple, compliant solutions are feasible resulting in different mixes of TOE and environmental contributions

In a specific CS2 "compliant"PP, the TOE (as a subset of the overall, notional CS2 system) may not provide support for some of these objectives. In that case such objectives would be moved into Table 4-1 (environmental objectives) for that PP. It is also possible that PP author may decide to specify the nature of compliant solutions more stringently than this CS2 PP guidance has done. It that case some of the joint objectives may become either a TOE objective and be moved into Table 4-2 (TOE objectives) ~~or ,~~ an environmental objective and be moved into Table 4-1 (environmental objectives), or a pair of objectives (one for the environment and one for the TOE). (These changes must be consistent with the threat categorizations in section 3.4 "Threats to Security"of the "compliant"PP.)

Table 4-3 –Joint TOE/Environment Security Objectives

Joint Security Objective	Corresponding Threat or Policy
O.ACCESS-MALICIOUS: The TOE controls will help in achieving this objective, but will not be sufficient. Additional, environmental controls are required to sufficiently mitigate the threat of malicious actions by authenticated users. This will be accomplished by focusing on deterrence, detection, and response with a goal of moderate effectiveness.	T.ACCESS-MALICIOUS
O.COMPLY: The TOE environment, in conjunction with controls implemented by the TOE, must support full compliance with applicable laws, regulations, and contractual agreements. This will be accomplished via some technical controls, yet with a focus on non-technical controls to achieve this objective with high effectiveness.	P.COMPLY
O.DETECT-SYSTEM: The TOE, in conjunction with other IT in the system, must enable the detection of system insecurities. The goal is high effectiveness for lower grade attacks.	P.SURVIVE T.SYSTEM-CORRUPTED
O.DUE-CARE: The TOE environment, in conjunction with the TOE itself, must be implemented and operated in a manner that clearly demonstrates due-care and diligence with respect to IT-related risks to the organization. This will be accomplished via a combination of technical and non-technical controls to achieve this objective with high effectiveness.	P.DUE-CARE

O.INFO-FLOW: The system IT (TOE and other IT), in conjunction with non-IT environmental controls, must ensure that any information flow control policies are enforced - (1) between system components and (2) at the system external interfaces.	P.INFO-FLOW
O.MANAGE: Those responsible for the TOE (in conjunction with mechanisms provided by the TOE) must ensure that it is managed and administered in a manner that maintains IT security. This will be accomplished with moderate effectiveness.	T.ADMIN-ERROR
O.NETWORK: The system must be able to meet its security objectives in a distributed environment. This will be accomplished with high effectiveness.	P.NETWORK
O.OPERATE: Those responsible for the TOE (in conjunction with mechanisms provided by the TOE) must ensure that the TOE is delivered, installed, and operated in a manner which maintains IT security. This will be accomplished with moderate effectiveness.	T.INSTALL T.OPERATE P.TRAINING
O.RECOVER-SYSTEM: The system must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecurity. This will be accomplished with some prevention and a majority of detect and respond, with high effectiveness for specified failures. For general failure, this will be accomplished with low effectiveness.	P.SURVIVE T.CRASH-SYSTEM

4.

Functional Security REQUIREMENTS

This section contains the functional requirements that must be satisfied by the notional CS2 system. A specific CS2 compliant PP will tailor these requirements to the specifics of the operational environment being addressed and the nature of the TOE within that environment. These requirements consist of functional components from Part 2 of the CC, in some cases with modifications.

This protection profile (PP) guidance is designed to be largely policy-neutral. Therefore, most policy-related assignments and selections are deferred to the PP for explicit specification. Where the policy is sufficiently generic, it is specified in this PP guidance and not deferred.

4.1 Functional Requirements - TOE

Table 5-1 lists the functional requirements for the notional CS2 information system and the security objectives each requirement helps to address. All functional and assurance dependencies associated with the components in Table 5-1 have been satisfied.

Appendix B contains the explicit functional requirements that are summarized here.

As described in sections 3.4 “Threats to Security”and 4. “Security Objectives”, for a specific, CS2 “compliant”PP, some of the system security needs will not be met by the TOE of that PP. As indicated in section 5.3, these unmet IT requirements become requirements on the IT environment surrounding the TOE and are moved from Table 5-1 into Table 5-2. (The requirements moved from Table 5-1 into Table 5-2 must correspond with the changes made to the CS2 guidance categorization of threats and objectives in sections 3.4 and 4 of the “compliant”PP.)

Table 5-1 –Functional Components - TOE

Req Number	CC Component	Name	Extended	Refined	PP/ST Detail - detail PP/ST adds detail	Objectives function helps address

					t a il	
1	FAU_GEN.1-CS2	Audit data Generation	x		x	O.Account-TOE O.Recover-TOE O.RECOVER-SYSTEM O.Detect-TOE O.DETECT-SYSTEM o.operate o.manage o.due-care
2	FAU_GEN.2	User Identity Generation		x		o.account-TOE
3	FAU_SAR.1	Audit Review			x	Required dependency for: FAU_SAR.2 FAU_SAR.3
4	FAU_SAR.2	Restricted Audit Review				O.bypass-TOE
5	FAU_SAR.3	Selectable Audit Review			x	o.account-TOE o.recover-TOE O.RECOVER-SYSTEM o.detect-TOE O.DETECT-SYSTEM o.due-care o.operate o.manage o.comply
6	FAU_SEL.1-CS2	Selective Audit	x	x	x	o.due-care o.detect-TOE O.DETECT-SYSTEM o.manage o.operate o.comply
7	FAU_STG.1	Protected audit trail storage		x		o.detect-TOE O.DETECT-SYSTEM o.due-care o.comply o.account-toe o.bypass-toe
8	FAU_STG.3	Action in case of Possible Audit Data Loss			x	o.account-toe o.due-care o.manage
9	FDP_ACC.1	Subset Access Control			x	o.access-toe o.ACCESS-MALICIOUS o.entry-toe o.due-care o.comply

						o.available-toe o.resources-TOE
10	FDP_ACF.1-CS2	Security Attribute Based Access Control	x		x	o.access-TOE O.ACCESS-MALICIOUS o.entry-TOE o.due-care o.comply o.available-TOE o.resources-TOE
11	FDP_DAU.1	Basic data authentication			x	o.bypass-toe o.due-care o.entry-toe o.available-toe
12	FDP_ETC.1-CS2	Export of user data without security attributes	x		x	o.bypass-TOE o.due-care o.entry-TOE o.available-TOE
13	FDP_IFC.1	Subset information flow control			x	Required dependency for: FDP_IFF.1 FDP_IFF.8
14	FDP_IFF.1	Simple security attributes			x	o.info-flow o.comply o.due-care
15	FDP_ITC.1	Import of user data without security attributes			x	o.network
16	FDP_ITT.1	Basic internal transfer protection			x	o.network
17	FDP_RIP.1	Subset Residual Information protection			x	o.bypass-TOE o.due-care
18	FDP_SDI.1	Stored data integrity monitoring			x	o.detect-TOE O.DETECT-SYSTEM o.recover-TOE o.recover-system
19	FDP_UCT.1	Basic data exchange confidentiality		x	x	o.network
20	FDP_UIT.1	Data exchange integrity		x	x	o.network
21	FIA_AFL.1	Authentication Failure Handling		x	x	o.detect-TOE O.DETECT-SYSTEM o.entry-toe o.bypass-toe o.due-care o.comply
22	FIA_ATD.1	User Attribute Definition			x	o.authorize-TOE
23	FIA_SOS.1	Verification of Secrets			x	o.bypass-TOE o.due-care o.comply
24	FIA_SOS.2	TSF Generation of Secrets			x	o.bypass-TOE

						o.due-care o.comply
25	FIA_UAU.1	Timing of authentication			x	o.known-TOE
26	FIA_UAU.5	Multiple authentication mechanisms			x	o.network
27	FIA_UAU.6	Re-authenticating			x	o.bypass-TOE
28	FIA_UAU.7	Protected authentication feedback				o.bypass-TOE
29	FIA_UID.1	Timing of identification			x	o.known-TOE
30	FIA_USB.1	User-Subject Binding				o.access-TOE O.ACCESS-MALICIOUS o.due-care o.bypass-TOE
31	FMT_MOF.1	Management of security functions behavior			x	o.manage o.due-care
32	FMT_MSA.1	Management of security attributes		x	x	o.manage o.due-care o.authorize-TOE
33	FMT_MSA.3	Static attribute initialization			x	o.manage o.due-care o.authorize-TOE
34	FMT_MTD.1	Management of TSF data		x	~~x~~	o.manage o.due-care
35	FMT_SAE.1	Time-Limited Authorization			x	o.access-TOE O.ACCESS-MALICIOUS o.entry-TOE o.authorize-TOE o.manage o.due-care
36	FMT_SMR.1	Security roles			x	o.manage o.due-care
37	FPT_AMT.1	Abstract Machine Testing		x	x	Required dependency for: FPT_TST.1
38	FPT_FLS.1	Failure with preservation of secure state			x	o.recover-TOE O.RECOVER-SYSTEM
39	FPT_ITC.1-CS2	Inter-TSF Confidentiality During Transmission	x	~~x~~	x	o.network
40	FPT_ITI.1-CS2	Inter-TSF detection of modification	x	~~x~~	x	o.network
41	FPT_ITT.1-CS2	Basic internal TSF data transfer protection	x	~~x~~	x	o.network
42	~~FPT_RCV.1~~FPT_RCV.2	~~Manual~~ Automated Recovery				o.recover-TOE O.RECOVER-SYSTEM
43	FPT_RPL.1	Replay detection			x	o.network
44	FPT_RVM.1	Non-Bypassability of the TSP				o.bypass-TOE
45	FPT_SEP.1	TSF Domain Separation				o.bypass-TOE o.due-care
46	FPT_TDC.1	Inter-TSF basic TSF data consistency		x	x	o.network

47	FPT_TRC.1	Internal TSF consistency			x	o.network
48	FPT_TST.1	TSF Testing		x	x	o.detect-TOE O.DETECT-SYSTEM o.due-care
49	~~FRU_RSA.1~~FRU_RSA.1-CS2	Maximum quotas			x	o.resources-TOE
50	FTA_LSA.1	Limitation on scope of selectable attributes			x	o.access-TOE O.ACCESS-MALICIOUS o.entry-TOE o.due-care
51	FTA_MCS.1-CS2	Basic limitation on multiple concurrent session	x	x	~~x~~	o.access-TOE O.ACCESS-MALICIOUS o.entry-TOE o.due-care
52	FTA_SSL.1	TSF-initiated session locking		~~x~~		o.bypass-TOE o.due-care
53	FTA_SSL.2	User-initiated locking				o.operate o.bypass-TOE o.due-care
54	FTA_SSL.3	TSF-initiated termination		~~x~~		o.bypass-TOE o.due-care
55	FTA_TAB.1-CS2	Default TOE access banners	x	~~x~~		o.entry-TOE o.account-TOE o.due-care o.comply
56	FTA_TAH.1	TOE access history				o.observe-TOE o.entry-TOE o.bypass-TOE o.due-care o.comply
57	FTA_TSE.1	TOE session establishment		~~x~~	x	o.access-TOE O.ACCESS-MALICIOUS o.entry-TOE
58	FTP_ITC.1-CS2	Inter-TSF trusted channel	x	~~x~~	x	o.network
59	FTP_TRP.1-CS2	Trusted path	x	~~x~~	x	o.network
60	Non-CC FPT_SYN-CS2.1	TSF synchronization FPT_STM.1 changed to be synchronization requirements (instead of just requiring a mechanism that supports it)	x			o.network

functional requirements - IT Environment
This section describes what is known about the functional requirements that the IT in the environment surrounding the TOE must provide in order for the environmental and joint security objectives to be met.

Since the TOE for this CS2 PP guidance document is the entire, notional CS2 system ~~- -~~ , the 'Non-TOE' objectives are null and Table 5-2 is ~~currently empty~~redundant for the notional TOE of this guidance document. However, in a specific, CS2 "compliant"PP the TOE will be a subset of the overall IT and this section will provide the requirements which must be met by the IT surrounding the TOE. The 'Non-TOE' objectives will then have meaning, driving expectations toward the IT other than the TOE. ~~This~~ Additionally a specific TOE might not be expected to provide all the functionality currently listed in Table 5-2, in which case the requirements that do not apply would be removed from Table 5-1.~~is be accomplished by moving the requirements from Table 5-1 which are not met by the TOE of that PP into Table 5-2 below.~~ (The requirements moved from Table 5-1 into Table 5-2 must correspond with the changes made to the CS2 guidance categorization of threats and objectives in sections 3.4 and 4 of the "compliant"PP.)

Table 5-2 –Functional Components - IT Environment

Req Number	CC Component	Name	Objectives function helps address
1	FAU_GEN.1-CS2	Audit data Generation	O.Account-non-TOE O.RECOVER-SYSTEM O.DETECT-SYSTEM o.operate o.manage o.due-care
2	FAU_GEN.2	User Identity Generation	o.account-non-TOE
3	FAU_SAR.1	Audit Review	Required dependency for: FAU_SAR.2 FAU_SAR.3
4	FAU_SAR.2	Restricted Audit Review	O.bypass-non-TOE
5	FAU_SAR.3	Selectable Audit Review	o.account-non-TOE O.RECOVER-SYSTEM O.DETECT-SYSTEM o.due-care o.operate o.manage o.comply
6	FAU_SEL.1-CS2	Selective Audit	o.due-care O.DETECT-SYSTEM o.manage o.operate o.comply

7	FAU_STG.1	Protected audit trail storage	O.DETECT-SYSTEM o.due-care o.comply o.account-non-toe o.bypass-non-toe
8	FAU_STG.3	Action in case of Possible Audit Data Loss	o.account-non-toe o.due-care o.manage
9	FDP_ACC.1	Subset Access Control	o.access-non-toe o.ACCESS-MALICIOUS o.entry-non-toe o.due-care o.comply o.available-non-toe o.resources-non-toe
10	FDP_ACF.1-CS2	Security Attribute Based Access Control	o.access-non-TOE O.ACCESS-MALICIOUS o.entry-non-TOE o.due-care o.comply o.available-non-TOE o.resources-non-toe
11	FDP_DAU.1	Basic data authentication	o.bypass-non-toe o.due-care o.entry-non-toe o.available-non-toe
12	FDP_ETC.1-CS2	Export of user data without security attributes	o.bypass-non-TOE o.due-care o.entry-non-TOE o.available-non-TOE
13	FDP_IFC.1	Subset information flow control	Required dependency for: FDP_IFF.1 FDP_IFF.8
14	FDP_IFF.1	Simple security attributes	o.info-flow o.comply o.due-care
15	FDP_ITC.1	Import of user data without security attributes	o.network
16	FDP_ITT.1	Basic internal transfer protection	o.network
17	FDP_RIP.1	Subset Residual Information protection	o.bypass-non-TOE o.due-care
18	FDP_SDI.1	Stored data integrity monitoring	O.DETECT-SYSTEM o.recover-system
19	FDP_UCT.1	Basic data exchange confidentiality	o.network
20	FDP_UIT.1	Data exchange integrity	o.network

21	FIA_AFL.1	Authentication Failure Handling	O.DETECT-SYSTEM o.entry-non-toe o.bypass-non-toe o.due-care o.comply
22	FIA_ATD.1	User Attribute Definition	o.authorize-non-TOE
23	FIA_SOS.1	Verification of Secrets	o.bypass-non-TOE o.due-care o.comply
24	FIA_SOS.2	TSF Generation of Secrets	o.bypass-non-TOE o.due-care o.comply
25	FIA_UAU.1	Timing of authentication	o.known-non-TOE
26	FIA_UAU.5	Multiple authentication mechanisms	o.network
27	FIA_UAU.6	Re-authenticating	o.bypass-non-TOE
28	FIA_UAU.7	Protected authentication feedback	o.bypass-non-TOE
29	FIA_UID.1	Timing of identification	o.known-non-TOE
30	FIA_USB.1	User-Subject Binding	o.access-non-TOE O.ACCESS-MALICIOUS o.due-care o.bypass-non-TOE
31	FMT_MOF.1	Management of security functions behavior	o.manage o.due-care
32	FMT_MSA.1	Management of security attributes	o.manage o.due-care o.authorize-non-TOE
33	FMT_MSA.3	Static attribute initialization	o.manage o.due-care o.authorize-non-TOE
34	FMT_MTD.1	Management of TSF data	o.manage o.due-care
35	FMT_SAE.1	Time-Limited Authorization	o.access-non-TOE O.ACCESS-MALICIOUS o.entry-non-TOE o.authorize-non-TOE o.manage o.due-care
36	FMT_SMR.1	Security roles	o.manage o.due-care
37	FPT_AMT.1	Abstract Machine Testing	Required dependency for: FPT_TST.1
38	FPT_FLS.1	Failure with preservation of secure state	O.RECOVER-SYSTEM
39	FPT_ITC.1-CS2	Inter-TSF Confidentiality During Transmission	o.network

40	FPT_ITI.1-CS2	Inter-TSF detection of modification	o.network
41	FPT_ITT.1	Basic internal TSF data transfer protection	o.network
42	FPT_RCV.2	Automated Recovery	O.RECOVER-SYSTEM
43	FPT_RPL.1	Replay detection	o.network
44	FPT_RVM.1	Non-Bypassability of the TSP	o.bypass-non-TOE
45	FPT_SEP.1	TSF Domain Separation	o.bypass-non-TOE o.due-care
46	FPT_TDC.1	Inter-TSF basic TSF data consistency	o.network
47	FPT_TRC.1	Internal TSF consistency	o.network
48	FPT_TST.1	TSF Testing	O.DETECT-SYSTEM o.due-care
49	FRU_RSA.1-CS2	Maximum quotas	o.resources-non-toe
50	FTA_LSA.1	Limitation on scope of selectable attributes	o.access-non-TOE O.ACCESS-MALICIOUS o.entry-non-TOE o.due-care
51	FTA_MCS.1-CS2	Basic limitation on multiple concurrent session	o.access-non-TOE O.ACCESS-MALICIOUS o.entry-non-TOE o.due-care
52	FTA_SSL.1	TSF-initiated session locking	o.bypass-non-TOE o.due-care
53	FTA_SSL.2	User-initiated locking	o.operate o.bypass-non-TOE o.due-care
54	FTA_SSL.3	TSF-initiated termination	o.bypass-non-TOE o.due-care
55	FTA_TAB.1-CS2	Default TOE access banners	o.entry-non-TOE o.account-non-TOE o.due-care o.comply
56	FTA_TAH.1	TOE access history	o.observe-non-TOE o.entry-non-TOE o.bypass-non-TOE o.due-care o.comply
57	FTA_TSE.1	TOE session establishment	o.access-non-TOE O.ACCESS-MALICIOUS o.entry-non-TOE
58	FTP_ITC.1-CS2	Inter-TSF trusted channel	o.network
59	FTP_TRP.1-CS2	Trusted path	o.network
60	Non-CC FPT_SYN-CS2.1	TSF synchronization FPT_STM.1 changed to be	o.network

		synchronization requirements (instead of just requiring a mechanism that supports it)	

non-it Environmental Functional Requirements

The environment is required to satisfy the secure usage assumptions in Section 3.~~1~~2, ~~and to~~ meet all of the environmental security objectives outlined in section 4.1, and support the objectives in section 4.3. The specific, non-IT functional requirements are not identified in this PP. The higher-level objective statements are considered sufficient for determining the adequacy of non-IT environmental support.

To the extent that the non-IT environment surrounding the notional CS2 system is the same as that surrounding the TOE in a specific, CS2 "compliant"PP, the expectations toward the non-IT environment will not change from PP to PP.

The following objectives are covered, almost exclusively, by non-IT environmental controls:

O.ACCESS-NON-TECHNICAL

O.DENIAL-SOPHISTICATED

O.DETECT-SOPHISTICATED

O.ENTRY-NON-TECHNICAL

O.ENTRY-SOPHISTICATED

O.PHYSICAL

The following objectives receive significant coverage by non-IT environmental controls:

O.ACCESS-MALICIOUS

O.COMPLY

O.DUE-CARE

O.MANAGE

O.OPERATE

4.2

Strength of function (SOF)

This section is required by the Common Criteria and specifies the strength of function necessary to accomplish the intent of this PP. Both a minimum level for the PP as a whole and specific metrics for individual functions are provided.

Note that, while not probabilistic, SOF metrics have been given for FAU_STG.1, FDP_RIP.1, FMT_MTD.1, and FPT_SEP.1. This extension of the CC with respect to SOF, is being used as a convenient means of capturing all "strength" elements in a common location of the PP.

4.2.1 Minimum SOF Requirement

As the goal for CS2 is near-term achievable COTS, the appropriate minimum SOF level is BASIC.

4.2.2 Specific SOF Requirements - TOE

The specific required strength metrics for the functional components are given in Table 5-3.

Table 5-3 –SOF Metrics - TOE

#	CC Component	Name	Explicit SOF Metric
1	FAU_GEN.1-CS2	Audit data Generation	
2	FAU_GEN.2	User Identity Generation	
3	FAU_SAR.1	Audit Review	
4	FAU_SAR.2	Restricted Audit Review	
5	FAU_SAR.3	Selectable Audit Review	
6	FAU_SEL.1	Selective Audit	
7	FAU_STG.1	Protected audit trail storage	provide a hardware write-protected copy of audit trail
8	FAU_STG.3	Action in case of Possible Audit Data Loss	
9	FDP_ACC.1	Subset Access Control	
10	FDP_ACF.1-CS2	Security Attribute Based Access Control	
11	FDP_DAU.1	Basic data authentication	
12	FDP_ETC.1-CS2	Export of user data without security attributes	
13	FDP_IFC.1	Subset information flow control	
14	FDP_IFF.1	Simple security attributes	
15	FDP_ITC.1	Import of user data without security attributes	
16	FDP_ITT.1	Basic internal transfer protection	
17	FDP_RIP.1	Subset Residual Information protection	applications will take advantage of OS supplied mechanisms
18	FDP_SDI.1	Stored data integrity monitoring	MD5 or ~~equivalent~~ stronger checksums will be used for critical data elements
19	FDP_UCT.1	Basic data exchange confidentiality	support equivalent ~~of~~ or stronger: 1024 bit key exchange and triple DES (as

			well as weaker values as required by import/export restrictions)
20	FDP_UIT.1	Data exchange integrity	MD5 or ~~equivalent~~ stronger checksums will be used
21	FIA_AFL.1	Authentication Failure Handling	
22	FIA_ATD.1	User Attribute Definition	
23	FIA_SOS.1	Verification of Secrets	FIBS PUB 112
24	FIA_SOS.2	TSF Generation of Secrets	
25	FIA_UAU.1	Timing of authentication	
26	FIA_UAU.5	Multiple authentication mechanisms	
27	FIA_UAU.6	Re-authenticating	
28	FIA_UAU.7	Protected authentication feedback	
29	FIA_UID.1	Timing of identification	
30	FIA_USB.1	User-Subject Binding	
31	FMT_MOF.1	Management of security functions behavior	
32	FMT_MSA.1	Management of security attributes	
33	FMT_MSA.3	Static attribute initialization	
34	FMT_MTD.1	Management of TSF data	include operating system access controls in controlling access to TSF critical data
35	FMT_SAE.1	Time-Limited Authorization	
36	FMT_SMR.1	Security roles	
37	FPT_AMT.1	Abstract Machine Testing	
38	FPT_FLS.1	Failure with preservation of secure state	
39	FPT_ITC.1-CS2	Inter-TSF Confidentiality During Transmission	support equivalent of 1024 bit key exchange and triple DES (as well as weaker values as required by import/export restrictions)
40	FPT_ITI.1-CS2	Inter-TSF detection of modification	MD5 or ~~equivalent~~ stronger checksums will be used
41	FPT_ITT.1	Basic internal TSF data transfer protection	disclosure: support equivalent ~~of~~ or stronger: 1024 bit key exchange and triple DES (as well as weaker values as required by import/export restrictions) modification: MD5 or ~~equivalent~~ stronger checksums will be used
42	~~FPT_RCV.1~~FPT_RCV.2	~~Manual~~ Automated Recovery	
43	FPT_RPL.1	Replay detection	
44	FPT_RVM.1	Non-Bypassability of the TSP	
45	FPT_SEP.1	TSF Domain Separation	use underlying hardware ring structure to separate, at a

			minimum, kernel space from application space
46	FPT_TDC.1	Inter-TSF basic TSF data consistency	
47	FPT_TRC.1	Internal TSF consistency	
48	FPT_TST.1	TSF Testing	MD5 or stronger~~equivalent~~ checksums will be used
49	~~FRU_RSA.1~~FRU_RSA.1-CS2	Maximum quotas	
50	FTA_LSA.1	Limitation on scope of selectable attributes	
51	FTA_MCS.1-CS2	Basic limitation on multiple concurrent session	
52	FTA_SSL.1	TSF-initiated session locking	
53	FTA_SSL.2	User-initiated locking	
54	FTA_SSL.3	TSF-initiated termination	
55	FTA_TAB.1-CS2	Default TOE access banners	
56	FTA_TAH.1	TOE access history	
57	FTA_TSE.1	TOE session establishment	
58	FTP_ITC.1-CS2	Inter-TSF trusted channel	
59	FTP_TRP.1-CS2	Trusted path	
60	FPT_SYN-CS2.1	TSF synchronization	

4.2.3

Specific SOF Metrics - IT Environment

In a CS2 “compliant”PP, for each of the functional components listed in Table 5-2, the corresponding entry from Table 5-3 is moved or added, as appropriate, into Table 5-4 below.

Table 5-4 –SOF Metrics - IT Environment

#	CC Component	Name	Explicit SOF Metric

Assurance Requirements

~~{Editorial note: The set of assurances listed here have been validated as reasonable by several state-level audits of certification authority systems.}~~

The assurance requirements for CS2 are met by an augmented EAL2 that is henceforth termed evaluation assurance level –CS2 (EAL-CS2). EAL-CS2 stresses assurance through vendor actions that are within the bounds of current best-commercial-practice. EAL-CS2 provides, primarily via review of vendor supplied evidence, independent confirmation that these actions have been competently performed. EAL-CS2 also includes the following independent, third-party analysis: (1) confirmation of system generation and installation procedures, (2) verification that the system security state is not misrepresented, (3) verification of a sample of the vendor functional testing, (4) searching for obvious vulnerabilities, and (5) independent functional testing.

The assurance components for EAL-CS2 are summarized in Table 6-1. Appendix C gives the details of these assurance components. Table 6-2 lists those components of EAL-CS2 that augment EAL2 from part 3 of the CC.

Table 6-1 –EAL-CS2 Assurance Components

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.3	Authorization controls
	ACM_SCP.2	Problem tracking CM Coverage
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, Generation, and Start-up Procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive High-Level Design
	ADV_RCR.1	Informal Correspondence Demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator Guidance
	AGD_USR.1	User Guidance
Life Cycle Support	ALC_DVS.1	Identification of Security Measures
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing - High-Level Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_MSU.2	Validation of Analysis
	AVA_SOF.1	Strength of TOE Security Function Evaluation
		Developer vulnerability Analysis

	AVA_VLA.1	

Table 6-2 –EAL-CS2 augmentation to EAL-2

EAL2	~~CS2-~~ ~~EAL~~**EAL-CS2**	**Nature of Augmentation to EAL2**
ACM_CAP.2	ACM_CAP.3	requires a CM plan describe how plan is used provide evidence that CM is operating in accordance with plan configuration items are being effectively maintained only authorized changes are made to configuration items
none	ACM_SCP.2	CM documentation shows that CM system tracks TOE implementation design documentation test documentation user and administrator documentation CM documentation security flaws CM documentation describes how configuration items are tracked
none	ADV_SPM.1	provide an informal TOE security policy model that describes rules and characteristics of all policies that can be modeled. includes a rationale demonstrating consistency and completeness with respect to these policies show consistency and completeness between all security functions in the functional specification and the model
none	ALC_DVS.1	produce developmental security documentation that describes the security measures necessary {in the opinion of the developer} to provide, for the TOE design and implementation, what confidentiality and integrity the developer considers necessary provides evidence that these measures are being followed during TOE development and maintenance evaluator confirms that the security measures identified are being applied Note: The evaluator does not, at ALC_DVS.1, confirm that the list of security measures in adequate. That is added at the next higher component (ALC_DVS.2).
none	ALC_FLR.2	establish procedure for accepting and action upon user reports of security flaws document flaw remediation procedures describing procedures used to track security flaws describing methods to provide flaw information, corrections, and guidance to users requiring that description of and effect of flaw be provided requiring that corrective actions be identified and correction status be provided

		ensuring that reported flaws are corrected and corrections issued to users providing safeguards that any corrections do not introduce new flaws
ATE_COV.1	ATE_COV.2	requirement for developer analysis of test coverage changing, for correspondence between test coverage and the functional specification, “evidence … show”to “analysis … demonstrate” requirement that the coverage is ‘complete’
none	ATE_DPT.1	requirement for developer analysis of test depth depth sufficient to demonstrate operates in accordance with high-level design
none	AVA_MSU.2	requirements placed upon guidance documentation identify all possible modes of operation, their consequences and implications toward secure operation be complete, clear, consistent, and reasonable list all assumptions about the intended environment list all requirements for external security measures developer analysis of guidance documentation for completeness evaluator confirmation of analysis of documentation completeness

Application NOTES

4.1 Evaluation scope, depth, and rigor.

In lieu of extensive, independent analysis, CS2 intends the evaluator to:

a. Review developer supplied evidence to make a determination on:

   i) the competence of the vendor
   ii) the apparent correctness and completeness of the required security actions

b. Approach all requirements to ensure “all”, “any”, or “none”as generic CC requirements to be interpreted loosely when applied to this lower assurance evaluation.

c. Be consciously aware that there is a point at which more evaluation is not cost-effective; keeping in mind that CS2 is a lower assurance, lower cost, basic level of security.

This intention to limit independent analysis directly applies to the following assurance elements:

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

b. ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

c. ADV_IND.2.2E The evaluator shall test the TSF to confirm that the TSF operates as specified.

d. AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

e. AVA_MSU.2.4E The evaluator shall confirm that the analysis shows that guidance is provided for secure operation in all modes of operation of the TOE.

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

g. AMA_CAT.1.2E The evaluator shall confirm that the categorization of TOE components and tools, and the categorization scheme used, are appropriate and consistent with the evaluation results for the certified version.

5. rationale

The rationale for this PP guidance is found in [CS2-R].

6. references

[CC-V2] Common Criteria for Information Technology Security Evaluation, May 1998.

[CS2-R] Rationale for CS2 - Protection Profile Guidance for Near-Term COTS, version 0.~~4~~5, ~~date- TBD~~March 1999.

APPENDIX A: ACRONYMS

CC	Common Criteria [for IT Security Evaluation]
COTS	Commercial Off The Shelf
EAL	Evaluation Assurance Level
IT	Information Technology

NIST	National Institute of Standards and Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

APPENDIX B: fUNCTIONAL rEQUIREMENT dETAILS

Refinements used throughout functional elements:

. ST Assignment: Where there is the potential for ST specific assignment -

- the following has been added to the PP assignment:

  "sufficient information for the ST author to make a compliant, ST specific assignment"

- and the following ST assignment has been added:

  [ST assignment: as [allowed | required] by PP, {ST specific assignment}]

The ST assignment may be "required"by the PP. This is where the PP author expects ST details to impact this requirement. An ST assignment may also be "allowed"by the PP. When "allowed", the PP author does not require that the ST add detail, but perceives that it may and wants to specify the requirements imposed on that detail. In either case (required or allowed), the PP author is expected to provide the detail necessary to enable evaluation of ST compliance with the PP. Examples of each case are:

Required. Identifying TSF data to be protected is an example of "required" ST assignment. The PP author may know general descriptions of TSF data, but need to have the ST author specify ST specific TSF data meeting PP defined criteria. For this particular example, it is anticipated that if the ST author chose to make a "null"assignment, then the ST would have to justify that there is no ST specific data meeting the PP criteria.

Allowed. An example of an allowed ST assignment is where the PP author provides a list of authorized roles, but is willing to allow the ST author to identify additional roles that may be unique to this ST and suitable for this requirement. In this case, the ST would probably not have to justify a "null" assignment, but would have to justify any additional roles as within the bounds specified by the PP. The ST author may wish to specify an additional role if having this role as authorized facilitates other requirements placed on the TOE.

. ST Selection: A similar general refinement has been applied to the case of a potential ST selection. Here the initial PP choice may have been a selection or an assignment.

PP selection. Rather than selecting from CC choices, the PP author may choose to defer to the ST. For example, with FDP_RIP, the PP author may not care, at the PP level of abstraction, whether the mechanism performs before allocation or after deallocation. The PP might require that the ST explicitly state the choice made and justify that this choice is correct in light of the rest of the ST.

PP assignment. The PP author may choose to handle an assignment by generating a list of choices from which the ST author must select. An example of this is FAU_STG.3 where the PP author may generate a list of acceptable actions to be taken in the event of audit trail exhaustion. By letting the ST select from among allowable choices, the specific characteristics of the TOE can influence which action, or set of actions, is used.

Syntax for expressing operations:

Throughout this appendix the following terminology is used:

Completed operations:
Selection: either [**selection:** selection made] or [selection made]
Assignment: [**assignment:** assignment made]
Refinement: refinement made
Extension: either [**extension:** extension made] or title indicating following is an extension

Deferred operations are shown in italics, for example:
Deferred assignment: *[**assignment:** description of operation to be performed]*

·.1 CS2-OS Access Control Security Function Policy (SFP)

The TOE shall support the administration and enforcement of the an access control SFP that provides at least the equivalent of the following two capabilities described below, in accordance with the precedence rules indicated.

·.1.1 Discretionary Access Control

Subjects (human users operating through software processes and software processes running as system processes) will be granted access to objects (files) based upon authorizations associated with the object being accessed, the name of the subject requesting access, the type of access requested, and the nature of the access request.

Authorizations associated with each object define allowed accesses by:

Subject identification:
Multiple individuals with potentially different access authorizations
Multiple subject groups with potentially different access authorizations

Access type, with explicit allow or deny:
Read
Write

Execute

Nature of access:
Time of day
Port of entry

For each object, an explicit owning subject (or group of subjects) will be identified.

For each object, the assignment and management of authorizations will be the responsibility of the owner of that object and, if the implementation allows, other subjects may be explicitly granted the privilege of modifying the object's authorizations.

The system is allowed to provide a privileged user or user role that can bypass all access controls; for example the Unix 'root'or NT 'administrator'.

·.1.2Non-discretionary access controls

a. The ability of a software process to access key system resources; for example external ports, input output capabilities, and operating system data structures; will be restricted based upon the assigned processing level of the process within a multiple ring architecture of the underlying hardware platform. A compliant security target will include a definition of key resources and a justification for the operating system architecture, displaying how allocation of OS processes and user processes between ring levels enforces non-discretionary access controls to key resources.

b. System level access controls set by explicitly authorized users such as a security adminstrator, and not modifiable by the asset owner. These include controls related to:

Nature of access, for example:
Time of day
Port of entry

Authentication mechanism(s) required

·.1.3CS2 Access Control Precedence Rules

CS2-OS compliant TOEs will determine allowed access for a specific subject to a specific object according to these precedence of rules:

) If the requested mode of access is denied to that subject, deny access.

) If the requested mode of access is permitted to that subject, permit access.

) If the requested mode of access is denied to every group of which the user is a member, deny access

) If the requested mode of access is permitted to any group of which the user is a member, grant access

) If the requested mode of access is denied to public, deny access

) If the requested mode of access is permitted to public, grant access

) Else deny access.

.2

Audit (fau)

·.2.1FAU_GEN.1-CS2 Audit data generation

Dependencies: FPT_STM.1 (FPT_SYN-CS2.1)

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

a) Start-up and shutdown of the audit functions;

b) All auditable events relevant for the [**selection:** basic] level of audit; and

c) [~~PP~~ **assignment:** other auditable events specific to the ST design as listed in the following ST assignment (the ST author is required to provide a basic justification for the assignment made, to include "null")~~other auditable events and sufficient information for ST author to make a compliant, ST specific assignment~~]

d) [**ST assignment:** as required by the PP, other ST specific auditable events]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (human user/software process), 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:** and the identity of process acting on behalf of a user or of the system~~PP assignment: other audit relevant information and sufficient information for ST author to make a compliant, ST specific assignment] and [ST assignment: as required by the PP, other ST specific audit relevant information~~].

Extension:

> FAU_GEN.1-CS2.3~~-CS2~~ When the TSF provides application support it shall support an application program interface that allows a privileged application to append data to the security audit trail or to an application-specified alternative security audit trail.

·.2.2FAU_GEN.2 User identity generation

Dependencies: FAU_GEN.1, FIA_UID.1

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the individual identity of the user ~~[refinement:~~ or system process~~]~~ that caused the event.

Refinement: See text of FAU_GEN.2.1

·.2.3FAU_SAR.1 Audit review

Dependencies: FAU_GEN.1

FAU_SAR.1.1 The TSF shall provide [**assignment:** explicitly authorized user roles, user groups, or individually identified users~~PP assignment: authorized users and sufficient information for ST author~~

~~to make a compliant ST specific assignment] and [ST assignment: as allowed by the PP, ST specific authorized users~~] with the capability to read [**assignment:** all information in the audit records~~PP assignment: list of audit information and sufficient information for ST author to make a compliant, ST specific assignment] and [ST assignment: as required by the PP, list of audit information arising due to the specifics of the TOE design~~] from the audit records.

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

·.2.4FAU_SAR.2 Restricted audit review

Dependencies: FAU_SAR.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.

·.2.5FAU_SAR.3 Selectable audit review

Dependencies: FAU_SAR.1

FAU_SAR.3.1 The TSF shall provide the ability to perform [**selection:** searches, sorting, and ordering] of audit data based upon [**assignment:** at a minimum, date and time of the event, subject (user or process), type of event, and success or failure~~PP assignment: multiple criteria with logical relations and sufficient information for the ST author to make a compliant, ST specific assignment], [ST assignment: as allowed by PP, ST specific multiple criteria with logical relations~~].

Refinement: See text of FAU_SAR.3.1

·.2.6FAU_SEL.1-CS2 Selective audit

Dependencies: FAU_GEN.1
FMT_MTD.1

~~FAU_SEL.2~~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) [**selection:** Object identity, user identity, subject identity, host identity, and/or event type];
b) [**assignment:** success or failure]~~PP assignment: list of additional attributes and sufficient information for ST author to make a compliant, ST specific assignment] and [ST assignment: as required by PP, list of ST specific additional attributes] that audit selectivity is based upon~~.

~~FAU_SEL.2.2 The TSF shall provide only the [PP assuagement: authorized users and sufficient information for the ST author to a make compliant, ST specific assignment] [ST assignment: as allowed by PP, ST specific authorized users] with the ability to [select or display] which events are to be audited.~~

Extension:

FAU_SEL.1-CS2.2 The TSF shall provide only explicitly authorized user roles, user groups, or individually identified users with the ability to select or display which events are to be audited.

FAU_SEL.1-CS2.3 The TSF shall provide the capability of FAU_SEL.1-CS2.2 at any time during the operation of the TOE.

Refinement: See text of FAU_SEL.1.1

~~FAU_SEL.2.3-CS2 The TSF shall provide the capability of FAU_SEL.2.2 at any time during the operation of the TOE.~~

·.2.7 FAU_STG.1 Protected audit trail storage

Dependencies: FAU_GEN.1

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [**selection:** prevent and detect] modifications to the audit records.

Refinement: See text in FAU_STG.1.2

·.2.8 FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1

FAU_STG.3.1 The TSF shall take [**assignment:** the action to notify an identified user or console of the possible audit data loss~~PP assignment: actions to be taken in case of possible audit storage failure or list of acceptable actions from which the ST author can make a selection with requirements on how selection is to be performed] [ST selection: as allowed by PP, from PP supplied list of actions~~] if the audit trail exceeds [~~refinement~~**assignment:** an authorized user selectable, pre-defined limit]. ~~Refinement:~~

~~See text in FAU_STG.3.1~~

·.3 User Data Protection (fdp)

·.3.1 FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1

FDP_ACC.1.1 The TSF shall enforce the [**assignment:** CS2 access control SFP~~PP assignment: access control SFP~~] on [**assignment: /PP assignment:** list of subjects, objects, and operations among subjects and objects covered by the SFP and sufficient information for ST author to make a compliant, ST specific assignment*]* and *[***ST assignment:**as required by PP, list of ST specific subjects, objects, and operations among subjects and objects covered by the SFP*]*].

·.3.2FDP_ACF.1-CS2 Security attribute based access control

Dependencies: FDP_ACC.1, FMT_MSA.3

FDP_ACF.1.1 The TSF shall enforce the [**assignment:** CS2 access control SFP~~PP assignment: access control SFP~~] to objects based on [**assignment:** user/process identity, group membership,~~]~~[, subject privileges, and access restrictions such as the time-of-day and port-of-entry, if included in the object authorization information~~PP assignment: other security attributes and sufficient information for ST author to make a compliant, ST specific assignment], and [ST assignment: as allowed by PP, other ST specific security attributes~~].

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:** by checking the authorizations associated with the object for the entries of that subject~~PP assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects~~].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**assignment:** none~~PP assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects~~].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**assignment:** none~~PP assignment: rules, based on security attributes, that explicitly deny access of subjects to objects~~].

Extension:

~~FDB~~FDP_ACF.1-CS2.5~~-CS2~~ The TSF shall provide the capability to assign a user to be a member of more than one user group simultaneously.

FDP_ACF.1-CS2.6~~-CS2~~ The TSF shall enforce the rules for authorizing and denying access based upon the~~se precedence rules: [~~ CS2 precedence rules~~PP assignment: list of precedence rules for determining access or sufficient information on precedence needs for the ST author to make a compliant, ST specific assignment] and [ST assignment: as allowed by PP, ST specific precedence rules]~~.

~~Application note. Potential rules for controlling access include:~~

~~a) It shall be possible to permit or deny access for a specific user or group of users for a specific mode of access.~~

~~b) At least two modes of access, equivalent to read (observe) and write (modify) shall be defined.~~

~~c) It shall be possible to permit or deny access to public (or world) to apply in cases where no specific user or group identity applies~~

~~d) Precedence of rules:~~

~~1) If a mode of access is denied to a specific user identity, deny access.~~

~~) If a mode of access is permitted to a specific user identity, permit access.~~

~~) If a mode of access is denied to any group of which the user is a member, deny access~~

~~) If a mode of access is permitted to any group of which the user is a member, grant access~~

~~) If a mode of access is denied to public, deny access~~

~~6) If a mode of access is permitted to public, grant access~~

~~) Else deny access.~~

·.3.3FDP_DAU.1 Basic data authentication

Dependencies: None

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: *[*PP assignment:** list of objects or information types and sufficient information for ST author to make a compliant, ST specific assignment*]* and *[***ST assignment:**as required by PP, list of ST specific objects or information types*]*].

FDP_DAU.1.2 The TSF shall provide [**assignment: *[*PP assignment:** list of subjects and sufficient information for ST author to make a compliant, ST specific assignmen*t] and [***ST assignment:**as required by PP, list of ST specific subjects*]*] with the ability to verify evidence of the validity of the indicated information.

·.3.4FDP_ETC.1-CS2 Export of user data without security attributes

Dependencies: FDP_ACC.1 or- FDP_IFC.1

FDP_ETC.1.1 The TSF shall enforce the [**assignment:** CS2 access control SFP and *[***PP assignment:**~~access control SFP and/or~~ information flow control SFP*]*] when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

Extension:

FDP_ETC.1-CS2.3 The TSF shall shall provide for outgoing information channels, for example TCP port numbers, that are under the control of the TSF and for which general application programs do not have access, when exporting user data controlled under the SFP outside the TSC.

·.3.5FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1

FDP_IFC.1.1 The TSF shall enforce the [**assignment: *[*PP assignment:**information flow control SFP*]*] on [**assignment: *[*PP assignment:** list of subjects, objects and operations among subjects and objects covered by the SFP and sufficient information for ST author to make a compliant, ST specific assignme*nt], and [S***T assignment:**as required by PP, list of ST specific subjects, objects and operations among subjects and objects covered by the SFP*]*].

·.3.6FDP_IFF.1 Simple security attributes

Dependencies: FDP_IFC.1, FMT_MSA.3

FDP_IFF.1.1 The TSF shall enforce the [**assignment: /PP assignment:**information flow control SFP*/*] ~~to enforce at least~~based on the following types of subject and object security attributes [**assignment: /PP assignment:** minimum number and type of security attributes and sufficient information for ST author to make a compliant, ST specific assignme*nt] and [ST* **assignment:**as required by PP, the ST specific minimum number and type of security attributes*/*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and a controlled information via a controlled operation if the following rules hold [**assignment: /PP assignment:** for each operation, the security attribute-based relationship that must hold between subject and object security attributes and sufficient information for ST author to make a compliant, ST specific assig*nment] and [S***T assignment:**as required by PP, for each operation, any ST specific security attribute-based relationship that must hold between subject and object security attribute*/*].

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

FDP_IFF.1.4 The TSF shall enforce the following [**assignment: /PP assignment:**list of additional SFP capabilities*/*].

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

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

·.3.7FDP_ITC.1 Import of user data without security attributes

Dependencies: FDP_ACC.1 or/and FDP_IFC.1, FMT_MSA.3

FDP_ITC.1.1 The TSF shall enforce the [**assignment:** CS2 access control SFP and */***PP assignment:**~~access control SFP and/or~~ information flow control SFP*/*] when importing user data, controlled under the SFP, from outside the TSC.

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

FDP_ITC.1.3 The TSF shall enforce the following the following rules when importing user data controlled under the SFP from outside the TSC: [**assignment:** the TOE shall provide for incoming information channels, for example TCP port numbers, that are under the control of the TSF and for which general application programs do not have access~~PP assignment: additional importation control rules and sufficient information for ST author to make a compliant, ST specific assignment] and [ST~~

~~assignment: as required by PP, any ST specific additional importation control rules~~] ~~when importing user data controlled under the SFP from outside the TSC~~.

·.3.8FDP_ITT.1 Basic internal transfer protection

Dependencies: FDP_ACC.1 or/and FDP_IFC.1

FDP_ITT.1.1 The TSF shall enforce the [**assignment:** CS2 access control SFP and */***PP assignment:**~~access control SFP and/or~~ information flow control SFP*/*] to prevent the ***/PP selection:*** *disclosure,/* [**selection:** modification, loss of use] of user data when it is transmitted between physically-separated parts of the TOE.

·.3.9FDP_RIP.1 Subset residual information protection

Dependencies: None

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**assignment:** following ST selection (ST author must provide a basic justification for the selection made, indicating suitability in meeting CS2 design goals)~~PP assignment: allocation of the resource to, deallocation of the resource from or sufficient information to allow ST author to make a compliant selection]~~ ; */***ST selection:** as allowed by PP: allocation of the resource to, deallocation of the resource from*/*] the following objects [**assignment:** shared memory and file storage space and the items defined in the following ST assignment (for which the ST author must provide a basic justification, indicating the all ST specific objects have been included)~~PP assignment: list of objects and sufficient information for ST author to make a compliant ST specific assignment]~~; and */***ST assignment:**as required by PP, ST specific list of objects*/*].

·.3.10 FDP_SDI.1 Stored data integrity monitoring

Dependencies: None

FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for [**assignment:** integrity errors resulting from unintentional corruption by the system~~PP assignment: integrity errors and sufficient information for ST author to make a compliant, ST specific assignment] [ST assignment: as allowed by PP, ST specific integrity errors~~] on all objects, based on the following [**assignment:** ***[ST selection:*** *all user data, data for which integrity protection has been explicitly requested]*~~PP assignment: user data attributes and sufficient information for ST author to make a compliant ST specific assignment] [ST assignment: as required by PP, ST specific user data attributes~~].

·.3.11 FDP_UCT.1 Basic data exchange confidentiality

Dependencies: FTP_ITC.1 or FTP_TRP.1, FDP_ACC.1 or/and FDP_IFC.1

FDP_UCT.1.1 The TSF shall enforce the [**assignment:** CS2 access control SFP and */***PP assignment:**~~access control SFP and/or~~ information flow control SFP*/*] to be able to [**selection:** transmit and receive] objects in a manner protected from unauthorized disclosure.

Refinement: See text in FDP_UCT.1.1

·.3.12 FDP_UIT.1 Data exchange integrity

Dependencies: FTP_ITC.1 or FTP_TRP.1, FDP_ACC.1 or/and FDP_IFC.1

FDP_UIT.1.1 The TSF shall enforce the [**assignment:** CS2 access control SFP and *[***PP assignment:**~~access control SFP and/or~~ *information* flow control SFP*]*] to be able to [**selection:** transmit ~~or~~ and receive] user data in a manner protected from [**selection:** modification, deletion, insertion, ~~or~~ and replay] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [**selection:** modification, deletion, insertion, or replay] has occurred.

Refinement: See text in FDP_UIT.1.1 and FDP_UIT.1.2

·.4 Identification and Authentication (FIA)

·.4.1FIA_AFL.1 Authentication failure handling

Dependencies: FIA_UAU.1

FIA_AFL.1.1 The TSF shall detect when [**assignment:** an authorized user configurable number of] unsuccessful authentication attempts ~~[refinement:~~ over an authorized user configurable length of time~~]~~ occur related to [**assignment:** initial account login, re-authentication after initial login, and~~[~~, list of other events given in the following ST assignment (the ST author must include a basic justification that the ST assignment, including a "null" assignment, includes all events specific to the ST design that require authentication failure handling);~~PP assignment: list of other authentication events and sufficient information for ST author to make a compliant, ST specific assignment] and~~ *[S***T assignment:** as required by PP, list of ST specific authentication events*]*].

~~FAI~~FIA_AFL.1.2 After the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**assignment:** perform the following ST selected actions (ST author must make a non-null selection, but does not need to justify the selection made as any are acceptable): *[**ST selection:** disable the account (requiring it to be re-enabled by an authorized user), cause each subsequent logon attempt to be delayed for increasing periods of time up to a maximum number of additional attempts at which time the account is disabled pending authorized user action to re-enable, allow either option based a configuration choice by an authorized user]*]~~[PP assignment: list of actions required or list of acceptable choices from which ST author may select along with any requirements imposed on this selection] [ST selection: as allowed by PP, from PP author provided list of actions]~~.

Refinement: See text of FIA_AFL.1.1

·.4.2FIA_ATD.1 User attribute definition

Dependencies: None

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**assignment:** user name, authenticator and the following ST specific attributes required by the design of the ST (the ST author must provide a basic justification for the list specified, to include "null"):~~PP assignment: list of security attributes and sufficient information for a compliant ST assignment of ST specific attributes] and~~ *[***ST assignment:**as required by PP, list of ST specific security attributes*]*].

·.4.3FIA_SOS.1 Verification of secrets

Dependencies: None

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**assignment**: for passwords, the application note below and the requirements of FIPS PUB 112; for other secrets specific to the ST design, the metric called out in the following ST assignment (the ST author must include a basic justification that all ST specific secrets are covered and that the metric(s) given are appropriate for meeting CS2 design goals):~~PP assignment: a defined quality metric or sufficient information for ST author to make a compliant, ST specific assignment]~~ *[***ST assignment:**as ~~allowed~~ *required* by PP, a*ny*ST specific, defined quality metric*s]*].

Application note. Potential elements for security quality metric related to passwords include:

a. Passwords shall not be reusable by the same user identifier for a period of time that can be set by an authorized user.

b. The TSF shall not indicate to the user if he/she has chosen a password already associated with another user.

c. The TSF shall, by default, prohibit the use of null passwords during normal operation.

d. The TSF shall provide an algorithm for ensuring the complexity of user-entered passwords that meets the following requirements:

   i. Passwords shall meet a system-specifiable minimum length requirement. The default minimum length shall be eight characters.

   ii. The password complexity-checking algorithm shall be modifiable by the TSF. The default algorithm shall require passwords to include at least one alphabetic character, one numeric character, and one special character.

   iii. The TSF should provide a protected mechanism that allows systems to specify a list of excluded passwords (e.g., company acronyms, common surnames).

   iv. The TSF should prevent users from selecting a password that matches any of those on the list of excluded passwords.

·.4.4FIA_SOS.2 TSF generation of secrets

Dependencies: None

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet [**assignment:** for passwords the metrics in the application note below and for other secrets according to the following assignments: *[***PP assignment**: a defined quality metric or sufficient information for ST author to make a compliant, ST specific assignm*ent] [**ST assignment:** as allowed by PP, a ST specific, defined quality metric]*].

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for [**assignment:** *[***PP assignment**: list of TSF functions and sufficient information for ST author to make a compliant, ST specific assignme*nt] [S***T assignment:** as required by PP, a ST specific, list of TSF functions*]*].

Application note. ~~Potential e~~Elements for security quality metric related to automated password generation include:

a. The password generation algorithm shall generate passwords that are easy to remember (i.e., pronounceable).

b. The TSF should give the user a choice of alternative passwords from which to choose.

c. Passwords shall be reasonably resistant to brute-force password guessing attacks.

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

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

·.4.1FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1

FIA_UAU.1.1 The TSF shall allow [**assignment:** *[***PP assignment:**list of TSF mediated actions and sufficient information for ST author to make a compliant, ST specific assignme*nt] [S***T assignment:** as required by PP, ST specific list of TSF mediated actions*]*] on behalf of the user to be performed before the user is authenticated.

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

·.4.2FIA_UAU.5 Multiple authentication mechanisms

Dependencies: None

FIA_UAU.5.1 The TSF shall provide [**assignment:** the required use of authentication mechanisms other than only passwords, based upon access parameters such as time of day, port of entry, and user privilege~~PP assignment: list of multiple authentication mechanisms or sufficient information for the ST author to make a complaint assignment] [ST assignment: as allowed by PP, list of multiple authentication mechanisms~~] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**assignment:** parameters for selecting authenticators required, these parameters are to be specifiable by an explicitly specified set of users, enforcing least privilege on the basis of the following ST selection (the ST author must provide a basic justification for the selection made, indicating how it supports enforcement of least privilege):~~PP assignment: sufficient information for the ST author to make a compliant assignment~~] *[***ST assignment:**as required by PP, rules describing how the multiple authentication mechanisms provide authentication*]*].

·.4.3FIA_UAU.6 Re-authentication

Dependencies: None

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [**assignment:** re-establishing a session following session locking, request to change authentication secrets, ~~]~~ ~~[~~and the following ST supplied conditions specific to the ST design (the ST author must provide a basic justification for the list provided, including a "null" list, showing why it is complete): ~~PP assignment: list of other conditions under which re-authentication is required and sufficient information for ST author to make a compliant, ST specific assignment], and~~ *[***ST assignment:**as required by PP, list of other, ST specific conditions under which re-authentication is required*]*].

·.4.4FIA_UAU.7 Protected authentication feedback

Dependencies: FIA_UAU.1

FIA_UAU.7.1 The TSF shall ~~only~~ not provide [**assignment:** ~~no~~ any indication of success or failure ~~and no~~nor clear-text display of any secret authenticator] to the user while the authentication is in progress.

Refinement: See text in FIA_UAU.7.1.

·.4.5FIA_UID.1 Timing of identification

Dependencies: None

FIA_UID.1.1 The TSF shall allow [**assignment:** *[***PP assignment:** list of TSF-mediated actions and sufficient information for ST author to make a compliant, ST specific assignment~~]~~ *and* ~~[~~*[***ST assignment:**as required by PP, list of ST specific, TSF-mediated actions*]*] on behalf of the user to be performed before the user is identified.

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.

·.4.6FIA_USB.1 User-subject binding

Dependencies: FIA_ATD.1

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

·.5 Security management (fmt)

·.5.1FMT_MOF.1 Management of security functions behavior

Dependencies: FMT_SMR.1

FMT_MOF.1.1 The TSF shall restrict the ability to [**selection:** determine the behaviour of, disable, enable, modify the behavior of] the functions [**assignment:** included as requirements for CS2-OS and for which the common criteria indicates security management suggestions, and also all items listed in the following ST assignment (the ST author must provide a basic justification for the assignment made, to include "null"): *[**ST assignment:** as required by PP, list of ST functions and mechanisms resulting from specifics of the ST design]*] to [**assignment:** an explicitly specified set of users, enforcing least privilege on the basis of the following ST selection (the ST author must provide a basic justification for the selection made, indicating how it supports enforcement of least privilege): *[**ST selection:** security administrators, security administrator roles, both]*]. ~~The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behavior of] the functions [PP assignment: list of functions and potential modification and sufficient information for ST author to make a compliant assignment] and [ST assignment: as required by PP, list of ST specific functions and potential modification] to [PP assignment: the authorized identified roles and sufficient information for ST author to make a compliant, ST specific assignment] and [ST assignment: as allowed by PP, the ST specific authorized identified roles].~~

·.5.2FMT_MSA.1 Management of security attributes

Dependencies: FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1

FMT_MSA.1.1 The TSF shall enforce the [**assignment:** CS2 access control SFP] to restrict the ability to [**selection:** change_default, modify, delete] and [**assignment:** "null"] the security attributes [**assignment:** all attributes used to define the security state of the system, to control the security functionality, to make access control decisions, and those listed in the following ST assignment (the ST author must provide a basic justification for the completeness of the assignment): *[**ST assignment:** as required by PP, list of security attributes requiring management and arising from the specifics of the ST design]*] to [**assignment:** for discretionary attributes, the owner of the attribute; for both discretionary and non-discretionary attributes, an explicitly specified set of users, enforcing least privilege on the basis of the following ST selection (the ST author must provide a basic justification for the selection made, indicating how it supports enforcement of least privilege): *[**ST selection:** security administrators, security administrator roles, both]*]. See iteration for restriction on read access to authenticator values.

Iteration:

FMT_MSA.1.1 The TSF shall enforce the [**assignment:** CS2 access control SFP] to restrict the ability to [**selection:** query] [**assignment:** "null"] the security attributes [**assignment:** current and

past values of authenticators,] to [**assignment:** no users and only to software processes requiring this knowledge].

Application note: An example of a processes requiring this information is a password change function which will query for current password and must make a determination as to whether the password entered is correct.

Refinement: See text in first iteration of FMT_MSA.1.1
~~FMT_MSA.1.1 The TSF shall enforce the [PP assignment: access control SFP, information flow control SFP] to restrict the ability to [change_default, modify, and delete] and [PP selection: read] the values of the security attributes [PP assignment: list of security attributes and sufficient information for ST author to make a compliant, ST specific assignment] and [ST assignment: as required by PP, list of ST specific security attributes] to [PP assignment: the authorized identified roles and sufficient information for ST author to make a compliant, ST specific assignment] and [ST assignment: as allowed by PP, the ST specific authorized identified roles].~~

·.5.3FMT_MSA.3 Static attribute initialization

Dependencies: -FMT_MSA.1, FMT_SMR.1

FMT_MSA.3.1 The TSF shall enforce the [**assignment:** CS2 access control SFP and /**PP assignment:**~~access control SFP,~~ information flow control SFP*]* to provide [**assignment:** restrictive~~PP assignment: restrictive, permissive, other property~~] default values for object security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**assignment:** data object owner and other authorized users] to specify alternate initial values to override the default values when an object or information is created.

·.5.4FMT_MTD.1 Management of TSF data

Dependencies: FMT_SMR.1

FMT_MTD.1.1 The TSF shall restrict the ability to [**selection:** change_default, read, modify, delete, or clear] the [**assignment:** all internal TSF data structures that are security critical] to [**assignment:** software processes explicitly authorized to access this data~~PP assignment: list of TSF data and sufficient information for ST author to make a compliant, ST specific assignment] and [ST assignment: as required by PP, list of ST specific TSF data] to [PP assignment: the authorized identified roles and sufficient information for ST author to make a compliant, ST specific assignment] and [ST assignment: as allowed by PP, the ST specific authorized identified roles~~].

Refinement: See text in FMT_MTD.1.1

·.5.5FMT_SAE.1 Time-limited authorization

Dependencies: FMT_SMR.1, FMT_STM.1 (FMT_CS2.1)

FMT_SAE.1.1 The TSF shall restrict the ability to specify an expiration time for [**assignment:** user account and authenticators and (with justification by the ST author for assignment made, to include "null"), ~~PP assignment: list of security attributes for which expiration is to be supported and sufficient information for ST author to make a compliant, ST specific assignment]~~ *[***ST assignment:**as required by PP, list of ST specific security attributes for which expiration is to be supported*]* to [**assignment:** an explicitly specified set of users, enforcing least privilege on the basis of the following ST selection (the ST author must provide a basic justification that the selection enforces least privilege): ~~PP assignment: the authorized identified roles and sufficient information for ST author to make a compliant, ST specific assignment] and~~ *[***ST assignment:** as allowed by PP, the ST specific authorized identified roles*]*].

FMT_SAE.1.2 For each of these security attributes, TSF shall be able to [**assignment:** for user account - disable account and require administrator action to re-enable, for authenticators - require owner of authenticator to establish a new value before proceeding with authenticated action] and ~~PP assignment: list of actions to be taken for each security attribute and sufficient information for ST author to make a compliant, ST specific assignment] and~~ *[***ST assignment:**as required by PP, list of ST specific actions to be taken for each security attribute*]* after the expiration time for the indicated security attribute has passed.

·.5.6FMT_SMR.1 Security roles

Dependencies: FIA_UID.1

FMT_SMR.1.1 The TSF shall maintain the roles [**assignment:** privileged user (for example the equivalent of the Unix root) and/or the following set of ST specific roles that the ST author wishes to specify as not conflicting with CS2 goals and useful in implementing these goals (the ST author must provide a basic justification that the roles specified do not conflict with CS2 design goals):~~PP assignment: the authorized identified roles and sufficient information for ST author to make a compliant, ST specific assignment]~~ ~~and~~ *[**ST assignment:** as allowed by PP, the ST specific authorized identified roles]*].

FMT_SMR.1.2 The TSF shall be able to associate users the roles.

·.6 Protection of Trusted Security (FPT)

·.6.1FPT_AMT.1 Abstract machine testing

Dependencies: None

FPT_AMT.~~3~~1.1 The TSF shall run a suite of tests [**selection:** during initial start-up and at the request of ~~an~~ explicitly authorized security administrator(s) or security administrator role(s) ~~authorized user~~], *[**PP selection:** periodically during normal operation]*, [**assignment:** *[***PP assignment:** other conditions and sufficient information for ST author to make a compliant, ST specific assignment*]* and *[**ST assignment:** as allowed by PP, other, ST specific conditions]*] to demonstrate the correct operation of the security ~~functions~~ assumptions provided by the abstract machine which underlies the TSF.

Refinement: See text in FPT_AMT.1.1

·.6.2FPT_FLS.1 Failure with preservation of secure state

Dependencies: ADV_SPM.1

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [**assignment:** those indicated in the following ST assignment: ~~PP assignment: list of types of TSF failures and sufficient information for ST author to make a compliant, ST specific assignment] and~~ *[S***T assignment:** as required by PP, list of ST specific types of TSF failures*]*].

Application note:

It is not considered feasible to indicated in the PP the failure modes from which the TOE will be able to recover. Instead, the intent of this requirement is for the ST to provide an explicit list so that users of the TOE have a clear understanding of recoverable, verses potentially non-recoverable, failures.

·.6.3FPT_ITC.1-CS2 Inter-TSF confidentiality during transmission

Dependencies: None

FPT_ITC.1.1-CS2 The TSF shall protect ~~[refinement:~~ [**extension:** authentication information and other ST specific TSF data as identified in the following, required ST assignment (which must be justified in the ST as being complete):~~PP assignment: list of TSF data and sufficient information for ST author to make a compliant, ST specific assignment]~~ ~~and~~ *[***ST assignment:** as required by PP, list of ST specific TSF data*]*] transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

~~Refinement~~**Extension**: See text of FPT_ITC.1.1-CS2

·.6.4FPT_ITI.1-CS2 Inter-TSF detection of modification

Dependencies: None

FPT_ITI.1.1-CS2 The TSF shall provide the capability to detect modification of [~~refinement~~**extension:** *[***PP assignment:** list of TSF data and sufficient information for ST author to make a compliant, ST specific assignment*]* and *[***ST assignment:** as required by PP, list of ST specific TSF dat*a]*] data during transmission between TSF and a remote trusted IT product within the following metric: [**assignment:** *[***PP assignment**: a defined modification metric and sufficient information for ST author to make a compliant, ST specific assignment*]*, *[***ST assignment:** as allowed by PP, a ST specific, defined modification metric*]*].

FPT_ITI.1.2-CS2 The TSF shall provide the capability to verify the integrity of [~~refinement~~**extension:***[***PP assignment:** list of TSF data and sufficient information for ST author to make a compliant, ST specific assignment*]* and *[***ST assignment:** as required by PP, list of ST specific TSF data*]*] transmitted between the TSF and a remote trusted IT product and perform [**assignment:** *[***PP assignment:** list of actions to be taken or list of acceptable choices from which

ST author may select along with any requirements imposed on this selection*] [***ST selection:**as allowed by PP, from PP author provided list of actions*]]* if modifications are detected.

~~Refinement~~**Extension**: See text in FPT_ITI.1.1 and FPT_ITI.1.2

·.6.5FPT_ITT.1-CS2 Basic Internal TSF data transfer

Dependencies: None

FPT_ITT.1.1-CS2 The TSF shall protect TSF data from [**selection:** modification], *[**PP selection:** disclosure, ~~modification~~]* ~~and~~ [~~refinement~~**extension:** and *[**PP selection**:*deletion, replay*]*] when it is transmitted between separate parts of the TOE.

~~Refinement~~**Extension**: See text in FPT_ITT.1.1

·.6.6FPT_RCV.~~1~~ 2 ~~Manual~~ Automated recovery

Dependencies: ADV_SPM.1, AGD_ADM.1, FPT_TST.1

FPT_RCV.~~1~~2.1 ~~After~~ When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.2.2 For [**assignment:** those indicated in the following ST assignment: *[**ST assignment:** as required by PP, list of ST specific types of TSF failures]*], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

·.6.7FPT_RPL.1 Replay detection

Dependencies: None

FPT_RPL.1.1 The TSF shall detect replay for the following entities [**assignment:** *[**PP assignment:** list of identified entities and sufficient information for ST author to make a compliant, ST specific assignment]*-, *[**ST assignment:** as required by PP, list of ST specific identified entities]*].

FPT_RPL.1.2 The TSF shall perform [**assignment:** *[**PP assignment:** list of actions to be taken or list of acceptable choices from which ST author may select along with any requirements imposed on this selection]*-, *[**ST selection:** as allowed by PP, from PP author provided list of actions]*] when replay is detected.

·.6.8FPT_RVM.1 Non-bypassability of the TSP

Dependencies: None

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before ~~any security-related action~~each function within the TSC is allowed to proceed.

·.6.9FPT_SEP.1 TSF domain separation

Dependencies: None

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

·.6.10 FPT_TDC.1 Inter-TSF basic TSF data consistency

Dependencies: None

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [**assignment:** *[**PP assignment:** list of TSF data types and sufficient information for ST author to make a compliant, ST specific assignment], [**ST assignment:** as required by PP, list of ST specific TSF data types]*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [**assignment:** *[**PP assignment:** list of interpretation rules to be applied by the TSF* ~~and sufficient information for ST author to make a compliant, ST specific assignment], [ST assignment: as required by PP, list of ST specific interpretation rules to be applied by the TSF~~*]*] when interpreting the TSF data from another trusted IT product.

Refinement - added element, clarifying intent:

> FPT_TDC.1.3-CS2 The TSF shall support maintaining consistent ~~[PP assignment: list of TSF data types and sufficient information for ST author to make a compliant, ST specific assignment] [ST assignment: as required by PP, list of ST specific data types]~~ data between this TSF and another trusted IT product for the data items specified in FPT_TDC.1.1 in accordance with the rules specified in FPT_TDC.1.2.

·.6.11 FPT_TRC.1 Internal TSF consistency

Dependencies: FPT_ITT.1

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [**assignment:** *[**PP assignment:** list of SFs dependent on TSF data replication consistency]*].

·.6.12 FPT_TST.1 TSF testing

Dependencies: FPT_AMT.1

FPT_TST.1.1 The TSF shall run a suite of self tests [**selection:** during initial start-up and at the request of explicitly authorized security administrator(s) or security administrator role(s)~~an authorized user~~] and *[**PP selection:** periodically during normal operation]* and [~~PP assignment: list of other conditions at which self test should occur or list of acceptable choices from which ST author may select along with any requirements imposed on this selection] [ST selection: as allowed by PP, from PP author provided list of actions~~***assignment:** "null"*] to demonstrate the correct operation of the TSF.

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

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

Refinement: See text in FPT_TST.1.1

·.6.13 FPT_SYN-CS2.1 TSF synchronization

Non-CC component

Extension:

Not hierarchical to any other component.

Dependencies: None

FPT_SYN-CS2.1.1 The TSF shall provide the capability to synchronize distributed TSF elements and to associate audit event records produced by multiple TSF entities.

Application note: This component is similar to FPT_STM "Time stamps", but calls out the synchronization requirement instead of a specifying a mechanism (i.e., reliable time stamps") that could be used for that purpose.

·.7 Resource utilization (fru)

·.7.1~~FRU_RSA.1~~FRU_RSA.1-CS2 Maximum quotas

Dependencies: None

FRU_RSA.1.1-CS2 The TSF shall enforce maximum quotas ~~limiting the maximum quota~~ of the following resources: [**assignment:** ***[PP assignment:** controlled resources and sufficient information for ST author to make a compliant, ST specific assignment], [**ST assignment:** as required by PP, ST specific controlled resources]*] that [**selection:** an individual user, a defined group of users, ~~or a~~ subjects] can use ***[PP selection:** simultaneously, over a specified period of time]*.

·.8 TOE Access (FTA)

·.8.1FTA_LSA.1 Limitation on scope of selectable attributes

Dependencies: None

FTA_LSA.1.1 The TSF shall restrict the scope of the session security attributes [**assignment:** ***[PP assignment:*** *session security attributes and sufficient information for ST author to make a compliant, ST specific assignment]*, ***[ST assignment:*** *as required by PP, ST specific session security attributes]*], based on [**assignment:** ***[PP assignment:*** *attributes and sufficient information for ST author to make a compliant, ST specific assignment]*, ***[ST assignment:*** *as required by PP, ST specific attributes]*].

·.8.2FTA_MCS.1-CS2 Basic limitation on multiple concurrent sessions

Dependencies: FIA_UID.1

FTA_MCS.1.1-CS2 The TSF shall [~~refinement~~**extension:** enable an authorized user to select at TOE startup whether or not to] restrict the maximum number of concurrent sessions that belong to the same user ~~[refinement: and to select, if restricting is enabled, the maximum number of allowed sessions per user]~~.

FTA_MCS.1.2 ~~[~~refinement: If the TOE is to restrict the maximum number of concurrent sessions,~~]~~ the TSF shall enforce [~~refinement~~**assignment:** an authorized user selected maximum number of] sessions~~]~~ per user.

Refinement: See text in ~~FTA_MCS.1.1 and~~ FTA_MCS.1.2
Extension: See text in FTA_MCS.1.1-CS2

·.8.3FTA_SSL.1 TSF initiated session locking

Dependencies: FIA_UAU.1

FTA_SSL.1.1 The TSF shall lock an interactive session after [~~refinement~~**assignment:** an authorized user specified~~]~~ time interval of user inactivity] 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.

FTA_SSL1.2 The TSF shall require the following events to occur prior to unlocking the session: [**assignment:** user authentication].

~~Refinement: See text in FTA_SSL.1.1~~

·.8.1FTA_SSL.2 User-initiated locking

Dependencies: FIA_UAU.1

FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive sessions by:

a) clearing or over-writing display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other then unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: [**assignment:** user authentication].

·.8.1FTA_SSL.3 TSF-initiated termination

Dependencies: None

FTA_SSL.3.1 The TSF shall terminate an interactive session after [~~refinement~~**assignment:** an authorized user specified~~]~~ time interval of user inactivity].

~~Refinement: See text in FTA_SSL.3.1~~

·.8.2FTA_TAB.1-CS2 Default TOE access banners

Dependencies: None

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

Extension:

FTA_TAB.1-CS2.2~~-CS2~~ The TSF shall provide the capability for an authorized user to specify and subsequently modify the contents of this warning message.

·.8.3FTA_TAH.1 TOE access history

Dependencies: None

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.

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

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.

Refinement: See text in FTA_TAH.1.1 and FTA_TAH.1.2

·.8.4FTA_TSE.1 TOE session establishment

Dependencies: None

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [**assignment:** attributes that can be set by explicitly authorized security administrator(s) or security administrator role(s), including user identity, port of entry, time of day, day of the week, and *[**PP assignment:** list of other attributes and sufficient information for ST author to make a compliant, ST specific assignment]*, and *[**ST assignment:** as allowed by PP, ST specific attributes]*].
~~FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [refinement: an authorized user specified] attributes [including user identity, port of entry, time of day, day of the week,] [PP assignment: list of other attributes and sufficient information for ST author to make a compliant, ST specific assignment], and [ST assignment: as allowed by PP, ST specific attributes].~~

~~Refinement: See text in FTA_TSE.1.1~~

·.9 trusted path/channels (FTP)

·.9.1 FTP_ITC.1-CS2 Inter-TSF trusted channel

Dependencies: None

FTP_ITC.1.1-CS2 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the [~~refinement~~**extension**: *[**PP assignment:** list of data types and sufficient information for ST author to make a compliant, ST specific assignment], [**ST assignment:** as required by PP, list of ST specific data types]*] channel data from modification and [~~refinement~~**extension**: *[***PP assignment:** list of data types and sufficient information for ST author to make a compliant, ST specific assignment*]* and *[***ST assignment:**as required by PP, list of ST specific data types*]*] channel data from disclosure.

FTP_ITC.1.2 The TSF shall permit *[**PP selection:** the TSF, the remote trusted IT product]* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**assignment:** *[**PP assignment:** list of functions for which a trusted channel is required and sufficient information for ST author to make a compliant, ST specific assignment], [**ST assignment:** as required by PP, list of ST specific functions for which a trusted channel is required]*].

~~Refinement~~**Extension**: See text in FTP_ITC.1.1-CS2

·.9.2 FTP_TRP.1-CS2 Trusted path

Dependencies: None

FTP_TRP.1.1-CS2 The TSF shall provide a communication path between itself and *[**PP selection:** local, remote]* users that is logically distinct from other communications paths and provides assured identification of its end points and protection of the [~~refinement~~**extension**: *[***PP assignment:**list of data types and sufficient information for ST author to make a compliant, ST specific assignment*]* and *[**ST assignment:** as required by PP, list of ST specific data types]*] communicated data from modification and [~~refinement~~**extension**: *[***PP assignment:** list of data types and sufficient

information for ST author to make a compliant, ST specific assignment*]* and *[***ST assignment:**as required by PP, list of ST specific data types*]*] communicated data from disclosure.

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [**selection:** initial user authentication, ~~user re-authentication, and~~] [**assignment:** user re-authentication, and *[**PP assignment:** list of other services for which trusted path is required and sufficient information for ST author to make a compliant, ST specific assignment], [**ST assignment:** as required by PP, list of ST specific services for which a trusted path is required]*].

~~Refinement~~**Extension**: See text in FTP_TRP.1.1

A. Appendix C: ASSURANCE rEQUIREMENT dETAILS

A.1 Configuration Management (ACM)

A.1.1 ACM_CAP.3 Authorization controls

Dependencies: CM_SCP.1, ALC_DVS.1

Developer action elements:

ACM_CAP.3.1D The developer shall provide a reference for the TOE.
ACM_CAP.3.2D The developer shall use a CM system.
ACM_CAP.3.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C The TOE shall be labeled with its reference.
ACM_CAP.3.3C The CM documentation shall include a configuration list and a CM plan.
ACM_CAP.3.4C The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.3.5C The CM documentation shall describe the method used to uniquely identify the TOE configuration items.
ACM_CAP.3.6C The CM system shall uniquely identify all configuration items.
ACM_CAP.3.7C The CM plan shall describe how the CM system is used.
ACM_CAP.3.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.3.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.3.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

Evaluator action elements:

ACM_CAP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

A.1.2 ACM_SCP.2 Problem tracking CM coverage

Dependencies: ACM_CAP.3

Developer action elements:

ACM_SCP.2.1D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.
ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:

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

A.2 Delivery and operation (ADO)

Delivery and operation provides requirements for correct delivery, installation, generation, and start-up of the TOE.

A.2.1 ADO_DEL.1 Delivery procedures

Dependencies: None

Developer action elements:

ADO_DEL.1.1D The developer shall document the procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe the procedures which are necessary to maintain security when distributing versions of the TOE to a user site.

Evaluator action elements:

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

A.2.2 ADO_IGS.1 Installation, generation, and start-up procedures

Dependencies: AGD_ADM.1

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures to be used for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2E The evaluator shall confirm that the installation procedures result in a secure configuration.

A.3 Development (ADV)

A.3.1 ADV_FSP.1 Informal functional specification

Dependencies: ADV_RCR.1

Developer action elements:

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

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.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

A.3.2 ADV_HLD.1 Descriptive high-level design

Dependencies: ADV_FSP.1, ADV_RCR.1

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.
ADV_HLD.1.2C The high-level design shall be internally consistent.
ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.1.5C 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.1.6C The high-level design shall identify the interfaces of the subsystems of the TSF.
ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate an complete instantiation of the TOE security functional requirements.

A.3.3 ADV_RCR.1 Informal Correspondence Demonstration

Dependencies: None

Developer action elements:

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

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of 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 TSF representation.

Evaluator action elements:

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

A.3.4 ADV_SPM.1 Informal TOE security policy model

Dependencies: ADV_FSP.1

Developer action elements:

ADV_SPM.1.1D The developer shall provide an TSP model.
ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

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 there are no security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

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

A.4 Guidance documents (AGD)

A.4.1 AGD_ADM.1 Administrator guidance

Dependencies: ADV_FSP.1

Developer action elements:

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

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 TOE 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 security parameters under the control of the administrator indicating safe values as appropriate.
AGD_ADM.1.5C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.6C The administrator guidance shall be consistent with all other documents supplied for evaluation.
AGD_ADM.1.7C The administrator guidance shall describe all security requirements on the IT environment which are relevant to the administrator.

Evaluator action elements:

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

A.4.2 AGD_USR.1 User Guidance

Dependencies: ADV_FSP.1

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

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 describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including all assumptions about user behavior found in the statement of TOE security environment.
AGD_USR.1.5C The user guidance shall be consistent with all other documentation delivered for evaluation.
AGD_USR.1.6C The user guidance shall describe all security requirements on the IT environment which are relevant to the user.

Evaluator action elements:

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

A.5 Life Cycle Support (ALC)

A.5.1 ALC_DVS.1 Identification of security measures

Dependencies: None

Developer action elements:

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

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_DVS.1.2E The evaluator shall check whether the security measures are being applied.

A.5.2 ALC_FLR.2 Flaw reporting procedures

Dependencies: None

Developer action elements:

ALC_FLR.2.1D The developer shall document the flaw remediation procedures.
ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon user reports of security flaws and requests for corrections to those flaws.

Content and 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 that 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 procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.
ALC_FLR.2.6C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

Evaluator Action Elements:

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

A.6 Tests (ATE)

A.6.1 ATE_COV.2 –Analysis of coverage

Dependencies: ADV_FSP.1, ATE_FUN.1

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests 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.

Evaluator Actions:

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

A.6.2 ATE_DPT.1 Testing: High Level Design

Dependencies: ADV_HLD.1, ATE_FUN.1

Developer action elements:

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.2.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TOE operates in accordance with the high level design.

Evaluator action elements:

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

A.6.3 ATE_FUN.1 Functional Testing

Dependencies: None

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.

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 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 procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The test results in the test documentation 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 security function operates as specified.

Evaluator action elements:

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

A.6.4 ATE_IND.2 Independent Testing - Sample

Dependencies: ADV_FSP.1, AGD_USR.1, AGD_ADM.1, ATE_FUN.1

Developer action elements:

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

Content and presentation of evidence elements:

ATE_IND.2.1C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E The evaluator shall test the TSF to confirm that the TSF 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.

A.7 Vulnerability assessment (AVA)

A.7.1 AVA_MSU.2 Validation of Analysis

Dependencies: ADO_IGS.1, AGD_ADM.1, AGD_USR.1, ADV_FSP.1

Developer action elements:

AVA_MSU.2.1D The developer shall provide guidance documentation.
AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE, including operation following failure or operational error, their consequences and implications for maintaining secure operation.
AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.2.3.C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.2.5C The developer's analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements:

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to check that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.
AVA_MSU.2.4E The evaluator shall confirm that the analysis shows that guidance is provided for secure operation in all modes of operation of the TOE.

A.7.2 AVA_SOF.1 Strength of TOE Security Function Evaluation

Dependencies: ADV_FSP.1, ADV_HLD.1

Developer action elements:

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

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 minimum strength level defined in the PP/ST.
AVA_SOF.1.2C 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.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

A.7.3 AVA_VLA.1 Developer vulnerability analysis

Dependencies: ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.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 identified vulnerabilities.

This section facilitates composability by providing what detail is known about the functional requirements that must be meet by the IT surrounding the TOE. As the TOE for the CS2 guidance document is the entire IT system, this section is currently empty. In a "compliant" CS2 PP, this section would provide detailed, CC requirements for the IT surrounding the TOE.

Content and presentation of evidence elements:

AVA_VLA.1.1C The evidence shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.1.2E The evaluator shall conduct penetration testing, based on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

A.8 Maintenance of assurance (AMA)

None