NISTIR 6462

CSPP - Guidance for COTS Security Protection Profiles

(Formerly: CS2 - Protection Profile Guidance for Near-Term COTS)

Version 1.0

Gary Stoneburner

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institutes of Standards and Technology
Gaithersburg, MD 20899

December 1999

U.S. DEPARTMENT OF COMMERCE
William M. Daley, Secretary

TECHNOLOGY ADMINISTRATION
Dr. Cheryl L. Shavers, Under Secretary
of Commerce for Technology

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Raymond G. Kammer, Director

TABLE OF CONTENTS

SECTION **PAGE**

TABLE OF TABLES

TABLE **PAGE**

1. INTRODUCTION

1.1 IDENTIFICATION

Title: CSPP - Guidance for COTS Security Protection Profiles
(Formerly: CS2 – Protection Profile Guidance for Near-Term COTS)

Assurance level: EAL2 – augmented (EAL-CSPP)

Registration: <To be filled in upon registration>

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

1.2 OVERVIEW

Background

CSPP is the first release of what, in draft form, was titled *CS2 - Protection Profile Guidance for Near-Term COTS*. CS2 originally appeared as "Commercial Security 2"; one of three sample, operating system profiles included in the draft, US Federal Criteria and in early editions of the Common Criteria. All sample profiles were removed from more recent editions the CC and, over time, CS2 moved from an operating system profile to a system profile to a guidance document for commercial off the shelf (COTS) profiles.

Because of some confusion due to multiple, different instantiations of 'CS2', the title of this document has been changed from CS2 to CSPP.

Purpose

The purpose of CSPP 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; giving those requirements which are generally applicable to such systems. CSPP is not intended to fully specify all possible systems. Additional functionality may be needed to capture specific needs; for example those related to (among others) network switching systems, role-based access control (RBAC), smart-cards, public key infrastructure (PKI), and sector-unique needs.

CSPP accomplishes its 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. CSPP 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. CSPP 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. CSPP "compliant" PPs are suitable for the protection of information in real-world environments, both commercial and government.

- Within government environments, CSPP "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 CSPP "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, CSPP "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 assumptions that apply for CSPP "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
- competent security administration is performed
- business/mission process automation is implemented with due regard for what CSPP "compliant" PPs do not expect of their TOEs.

Summary of CSPP Requirements

Systems incorporating main-stream, COTS products achieve the advantages such products offer; for example, high-functionality with low-cost. However, these advantages are not achieved without some tradeoffs; an example of which is security capability. CSPP identifies a cost-effective, security baseline for systems built from COTS, ensuring that reasonable security expectations are achieved.

CSPP also identifies those areas where it is not realistic to expect a typical COTS product to provide sufficient protection. These areas are the direct result of the fact that the driving factors for COTS (functionality, cost, and time to market) have tended to work against increasing the security capabilities beyond those identified in CSPP.

Assurance. CSPP 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 malicious) authenticated users
- provide protection against unsophisticated, technical attacks
- can not be expected to adequately protect against sophisticated, technical attacks (to include denial-of-service)

Functionality. The notional CSPP 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

CSPP "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

2. 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 CSPP 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.

2.1 PRODUCT CLASS

CSPP 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.

2.2 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

2.3 REQUIRED SECURITY FUNCTIONALITY

CSPP specifies the requirements for a system with the security functionality listed below. A specific CSPP "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

3. SECURITY ENVIRONMENT

3.1 INTRODUCTION

This section identifies the following:

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

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.

3.2 SECURE USAGE ASSUMPTIONS

The specific conditions listed below are assumed to exist in a CSPP environment. These assumptions include both practical realities to be considered in the development of security requirements in CSPP "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. 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 CSPP 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"

3.3 ORGANIZATIONAL SECURITY POLICIES

The organizational security policies discussed below are addressed by the notional CSPP 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.	CSPP 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.	CSPP 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.	CSPP 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 CSPP systems will likely be interconnected across untrusted networking, this policy statement will have a significant impact on CSPP requirement definition.

Name	Policy	Discussion
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 insecurity, resisting the insecurity and/or providing the means to detect an insecurity and recover from it.	CSPP systems will provide a measure of this resilience through functionality and assurances that resist, 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.	CSPP systems must, in conjunction with its environment, ensure that the organization's information technology is not used for unauthorized purposes.

3.4 THREATS TO SECURITY

The technical countermeasures of the notional CSPP 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 CSPP 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 either addressed by the TOE's environment or risk accepted. This is done to facilitate the composition of a CSPP compatible system with the TOE of a given PP. Some of the threats in Table 3.4-1 are expected in every CSPP "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.

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 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

A CSPP "compliant" PP will tailor 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 CSPP system into Table 3.4-3 (jointly addressed threats). (In the CSPP "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	For audit trails under control of the TOE, records of security events may be disclosed to unauthorized individuals or processes.
T.AUDIT-CORRUPTED-TOE	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 CSPP "compliant" PP, the TOE (as a subset of the overall, notional CSPP 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 CSPP 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 CSPP "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 system, as a result of another threat, may be intentionally corrupted to enable future insecurities.

3.4.1 Threats environment addresses

The threats discussed below must be countered but are not addressed by the technical countermeasures within the notional CSPP system. Such threats must therefore, be addressed in conjunction with the operating environment. Note that a measure of explicit risk acceptance is frequently a viable option.

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. CSPP 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. CSPP 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 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.

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 system may be subjected to a physical attack that may compromise security.

The security offered by CSPP 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.

3.4.2 Threats TOE addresses

Technical countermeasures within the notional CSPP 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. CSPP 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. CSPP 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. 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 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 CSPP PP will resist low-grade technical attacks. (Resistance to higher-grade attacks, when such resistance is required, must be provided in conjunction with 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: Due to the TOE, security relevant events may not be traceable to the user or system process associated with the event.

3.4.3 Threats TOE and Environment jointly address

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

CSPP 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 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 system may be delivered or installed in a manner that undermines security.

The security offered by CSPP is predicated upon the 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 CSPP 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.

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.)

3.5 GENERAL ASSURANCE NEED

CSPP "compliant" PPs are targeted for near-term achievable, cost-effective, COTS security. In keeping with this target, the general level of assurance for CSPP 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.

CSPP assurance must also, to enhance wide-spread acceptance, be consistent with current and near-term mutual recognition arrangement. This requires that the CSPP 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 CSPP is EAL2 augmented to include other vendor actions within the scope of current best commercial practice.

4. SECURITY OBJECTIVES

4.1 ENVIRONMENTAL SECURITY OBJECTIVES

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

The purpose of the environmental objectives (in conjunction with the Joint objectives) is to state what is expected of the TOE's environment in terms of risk mitigation and explicit risk acceptance. This is done primarily to facilitate determining the security requirements which the environment must meet in order to compose a CSPP "compliant" system using the TOE of a given PP. Since a specific PP narrows the scope to a specific IT product within the system, that PP 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 CSPP 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.) Also note that if a threat is to be addressed in some measure by explicit risk acceptance, the corresponding objective(s) must be modified accordingly.

Table 4-1 – Environmental Security Objectives

Environmental Security Objective	Corresponding Threat or Policy
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

Environmental Security Objective	Corresponding Threat or Policy
O.AUTHORIZE-Non-TOE: The IT other than 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 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.	P.ACCESS
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 CSPP 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

Environmental Security Objective	Corresponding Threat or Policy
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

4.2 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 4-2 gives the security objectives to be met by the notional CSPP information system.

While all of the TOE objectives will be covered in a CSPP "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 CSPP 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

IT Security Objective	Corresponding Threat or Policy
O.BYPASS-TOE: The TOE must prevent errant or non-malicious, 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 CSPP controls are not expected to be sufficient mitigation for the greater negative impact that 'malicious' implies.	T.ACCESS-TOE
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.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.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.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

4.3 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 CSPP "compliant" PP, the TOE (as a subset of the overall, notional CSPP 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 CSPP 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), 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	P.DUE-CARE

Joint Security Objective	Corresponding Threat or Policy
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.	
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, but the majority of the focus will be on detection and response, with high effectiveness for specified failures. For general failure, this will be accomplished with low effectiveness.	P.SURVIVE T.CRASH-SYSTEM

5. FUNCTIONAL SECURITY REQUIREMENTS

This section contains the functional requirements that must be satisfied by the notional CSPP system. A specific CSPP 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 (for example, the policies listed in section 3.3), it is specified in this PP guidance and not deferred.

5.1 FUNCTIONAL REQUIREMENTS - TOE

Table 5-1 lists the functional requirements for the notional CSPP 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, CSPP “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 CSPP 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	PP/ST adds detail to PP detail	Objectives function helps address
1	FAU_GEN.1-CSPP	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

Req Number	CC Component	Name	Extended	Refined	PP/ST Detail	PP/ST adds detail to PP/ST detail	Objectives function helps address
3	FAU_SAR.1	Audit Review					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					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-CSPP	Selective Audit	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					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

Req Number	CC Component	Name	Extended	Refined	PP/ST Detail DeatailPP/ST adds detaildetailPP /ST detail	Objectives function helps address
10	FDP_ACF.1-CSPP	Security Attribute Based Access Control	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-CSPP	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

Req Number	CC Component	Name	Extended	Refined	PP/ST Detail	PP/ST DeatailPP/ST adds detailsdetailPP /ST detail	Objectives function helps address
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			O.MANAGE O.DUE-CARE

Req Number	CC Component	Name	Extended	Refined	PP/ST Detail DeatailPP/ST adds detailedDetailPP /ST detail	Objectives function helps address
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-CSPP	Inter-TSF Confidentiality During Transmission	x		x	O.NETWORK
40	FPT_ITI.1-CSPP	Inter-TSF detection of modification	x		x	O.NETWORK
41	FPT_ITT.1-CSPP	Basic internal TSF data transfer protection	x		x	O.NETWORK
42	FPT_RCV.2	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-CSPP	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

Req Number	CC Component	Name	Extended	Refined	PP/ST Detail	PP/ST adds detail to PP detail	Objectives function helps address
51	FTA_MCS.1-CSPP	Basic limitation on multiple concurrent session	x	x			O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.DUE-CARE
52	FTA_SSL.1	TSF-initiated session locking					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					O.BYPASS-TOE O.DUE-CARE
55	FTA_TAB.1-CSPP	Default TOE access banners	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		O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE
58	FTP_ITC.1-CSPP	Inter-TSF trusted channel	x		x		O.NETWORK
59	FTP_TRP.1-CSPP	Trusted path	x		x		O.NETWORK
60	Non-CC FPT_SYN-CSPP.1	TSF synchronization FPT_STM.1 changed to be synchronization requirements (instead of just requiring a mechanism that supports it)	x				O.NETWORK

5.2 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 CSPP PP guidance document is the entire, notional CSPP system, the 'Non-TOE' objectives are essentially null and Table 5-2 could therefore be empty. Instead this table contains the complete list of functions to facilitate its use as a template for CSPP "compliant" PPs, allowing the PP author to simply delete the requirements that do not apply. In a specific, CSPP "compliant" PP the TOE will be a subset of the overall IT and section 5.2 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. Additionally a specific TOE might not be expected to provide all the functionality currently listed in Table 5-1, in which case the requirements that do not apply would be removed from Table 5-1. (The requirements moved from Table 5-1 into Table 5-2 must correspond with the changes made to the CSPP 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-CSPP	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

Req Number	CC Component	Name	Objectives function helps address
6	FAU_SEL.1-CSPP	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-CSPP	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-CSPP	Export of user data without security attributes	O.BYPASS-NON-TOE O.DUE-CARE O.ENTRY-NON-TOE O.AVAILABLE-NON-TOE

Req Number	CC Component	Name	Objectives function helps address
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

Req Number	CC Component	Name	Objectives function helps address
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-CSPP	Inter-TSF Confidentiality During Transmission	O.NETWORK
40	FPT_ITI.1-CSPP	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

Req Number	CC Component	Name	Objectives function helps address
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-CSPP	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-CSPP	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-CSPP	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-CSPP	Inter-TSF trusted channel	O.NETWORK

Req Number	CC Component	Name	Objectives function helps address
59	FTP_TRP.1-CSPP	Trusted path	O.NETWORK
60	Non-CC FPT_SYN-CSPP.1	TSF synchronization FPT_STM.1 changed to be synchronization requirements (instead of just requiring a mechanism that supports it)	O.NETWORK

5.3 NON-IT ENVIRONMENTAL FUNCTIONAL REQUIREMENTS

The environment is required to satisfy the secure usage assumptions in Section 3.2, 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 CSPP system is the same as that surrounding the TOE in a specific, CSPP "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

5.4 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.

5.4.1 Minimum SOF Requirement

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

5.4.2 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-CSPP	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-CSPP	Security Attribute Based Access Control	—
11	FDP_DAU.1	Basic data authentication	—
12	FDP_ETC.1-CSPP	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	—

#	CC Component	Name	Explicit SOF Metric
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 stronger checksums will be used for critical data elements
19	FDP_UCT.1	Basic data exchange confidentiality	support equivalent 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 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-CSPP	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)

#	CC Component	Name	Explicit SOF Metric
40	FPT_ITI.1-CSPP	Inter-TSF detection of modification	MD5 or stronger checksums will be used
41	FPT_ITT.1	Basic internal TSF data transfer protection	disclosure: support equivalent or stronger: 1024 bit key exchange and triple DES (as well as weaker values as required by import/export restrictions) modification: MD5 or stronger checksums will be used
42	FPT_RCV.2	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 checksums will be used
49	FRU_RSA.1-CSPP	Maximum quotas	—
50	FTA_LSA.1	Limitation on scope of selectable attributes	—
51	FTA_MCS.1-CSPP	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-CSPP	Default TOE access banners	—
56	FTA_TAH.1	TOE access history	—
57	FTA_TSE.1	TOE session establishment	—
58	FTP_ITC.1-CSPP	Inter-TSF trusted channel	—
59	FTP_TRP.1-CSPP	Trusted path	—
60	FPT_SYN-CSPP.1	TSF synchronization	—

5.4.3 Specific SOF Metrics - IT Environment

In a CSPP "compliant" PP, for each of the functional components listed in the PP table corresponding to the Table 5-2 template, 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

6. ASSURANCE REQUIREMENTS

The assurance requirements for CSPP are met by an augmented EAL2 that is henceforth termed evaluation assurance level – CSPP (EAL-CSPP). EAL-CSPP stresses assurance through vendor actions that are within the bounds of current best-commercial-practice. EAL-CSPP provides, primarily via review of vendor supplied evidence, independent confirmation that these actions have been competently performed. EAL-CSPP 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-CSPP are summarized in Table 6-1. Appendix C gives the details of these assurance components. Table 6-2 lists those components of EAL-CSPP that augment EAL2 from part 3 of the CC.

Table 6-1 – EAL-CSPP 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
	AVA_VLA.1	Developer vulnerability Analysis

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

EAL2	EAL-CSPP	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).

EAL2	EAL-CSPP	Nature of Augmentation to EAL2
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

7. APPLICATION NOTES

7.1 EVALUATION SCOPE, DEPTH, AND RIGOR.

In lieu of extensive, independent analysis, CSPP 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 CSPP 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.

8. RATIONALE

The rationale for CSPP is an important part of the PP guidance, and is included at Appendix E. This appendix is formatted as if it were a separate document to facilitate its use as a template for a separate rationale document. Publishing the rationale separately is often desired as the audience for the rationale is smaller than that for the PP, and a separate rationale document greatly reduces the size of the base PP document.

9. REFERENCES

[CC-V2.1] *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999.

[CSPP-R] Rationale for *CSPP - Guidance for COTS Security Protection Profiles*, December 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

COMMON SYNTAX

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]*

Refinements used throughout functional elements:

1. 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.

2. 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.

CSPP-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.

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'.

Non-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

CSPP Access Control Precedence Rules

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

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

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

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

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

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

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

7) Else deny access.

AUDIT (FAU)

FAU_GEN.1-CSPP Audit data generation

Dependencies: FPT_STM.1 (FPT_SYN-CSPP.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) [**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")]

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:** the identity of the process acting on behalf of a user or of the system, and the subject's user group for this access].

Extension:

FAU_GEN.1-CSPP.3 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.

FAU_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 or system process that caused the event.

Refinement: See text of FAU_GEN.2.1

FAU_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] with the capability to read [**assignment:** all information in the audit records] 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.

FAU_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.

FAU_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].

Refinement: See text of FAU_SAR.3.1

FAU_SEL.1-CSPP Selective audit

Dependencies: FAU_GEN.1
FMT_MTD.1

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
a) [**selection:** Object identity, user identity, subject identity, host identity, and/or event type];
b) [**assignment:** success or failure].

Extension:

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

Refinement: See text of FAU_SEL.1.1

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

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] if the audit trail exceeds [**assignment:** an authorized user selectable, pre-defined limit].

USER DATA PROTECTION (FDP)

FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1

FDP_ACC.1.1 The TSF shall enforce the [**assignment:** CSPP 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]*].

FDP_ACF.1-CSPP Security attribute based access control

Dependencies: FDP_ACC.1, FMT_MSA.3

FDP_ACF.1.1 The TSF shall enforce the [**assignment:** CSPP 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].

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].

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

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

Extension:

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

FDP_ACF.1-CSPP.6 The TSF shall enforce the rules for authorizing and denying access based upon the CSPP precedence rules.

FDP_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 assignment] 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.

FDP_ETC.1-CSPP 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:** CSPP access control SFP and ***[PP assignment:*** *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-CSPP.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.

FDP_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 assignment], and [**ST assignment:** as required by PP, list of ST specific subjects, objects and operations among subjects and objects covered by the SFP]*].

FDP_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]*] 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 assignment] 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 assignment] and [**ST 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]*].

FDP_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:** CSPP access control SFP and *[**PP assignment:** 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].

FDP_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:** CSPP access control SFP and ***[PP assignment:*** *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.

FDP_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 CSPP design goals): ***[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): ***[ST assignment:*** *as required by PP, ST specific list of objects]*].

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] on all objects, based on the following [**assignment:** ***[ST selection:*** *all user data, data for which integrity protection has been explicitly requested]*].

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:** CSPP access control SFP and ***[PP assignment:*** *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

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:** CSPP access control SFP and ***[PP assignment:*** *information flow control SFP]*] to be able to [**selection:** transmit and receive] user data in a manner protected from [**selection:** modification, deletion, insertion, 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

IDENTIFICATION AND AUTHENTICATION (FIA)

FIA_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 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):*[**ST assignment:** as required by PP, list of ST specific authentication events]*].

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]*].

Refinement: See text of FIA_AFL.1.1

FIA_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"): *[**ST assignment:** as required by PP, list of ST specific security attributes]*].

FIA_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 CSPP design goals): *[**ST assignment:** as required by PP, any ST specific, defined quality metrics]*].

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

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

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

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

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

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

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.

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

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

FIA_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 assignment] [**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 assignment] [**ST assignment:** as required by PP, a ST specific, list of TSF functions]*].

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

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

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

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

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

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).

FIA_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 assignment] [**ST 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.

FIA_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] 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): *[**ST assignment:** as required by PP, rules describing how the multiple authentication mechanisms provide authentication]*].

FIA_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): *[**ST assignment:** as required by PP, list of other, ST specific conditions under which re-authentication is required]*].

FIA_UAU.7 Protected authentication feedback

Dependencies: FIA_UAU.1

FIA_UAU.7.1 The TSF shall not provide [**assignment:** any indication of success or failure 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.

FIA_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.

FIA_USB.1 User-subject binding

Dependencies: FIA_ATD.1

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

SECURITY MANAGEMENT (FMT)

FMT_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 CSPP-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]*].

FMT_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:** CSPP 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:** CSPP 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.3 Static attribute initialization

Dependencies: -FMT_MSA.1, FMT_SMR.1

FMT_MSA.3.1 The TSF shall enforce the [**assignment:** CSPP access control SFP and *[**PP assignment:** information flow control SFP]*] to provide [**assignment:** restrictive] 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.

FMT_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].

Refinement: See text in FMT_MTD.1.1

FMT_SAE.1 Time-limited authorization

Dependencies: FMT_SMR.1, FMT_STM.1 (FMT_CSPP.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"), *[**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): *[**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 *[**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.

FMT_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 CSPP goals and useful in implementing these goals (the ST author must provide a basic justification that the roles specified do not conflict with CSPP design goals): *[**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.

PROTECTION OF TRUSTED SECURITY (FPT)

FPT_AMT.1 Abstract machine testing

Dependencies: None

FPT_AMT.1.1 The TSF shall run a suite of tests [**selection:** during initial start-up and at the request of explicitly authorized security administrator(s) or security administrator role(s)], *[**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 assumptions provided by the abstract machine which underlies the TSF.

Refinement: See text in FPT_AMT.1.1

FPT_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: *[**ST 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.

FPT_ITC.1-CSPP Inter-TSF confidentiality during transmission

Dependencies: None

FPT_ITC.1.1-CSPP The TSF shall protect [**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): *[**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.

Extension: See text of FPT_ITC.1.1-CSPP

FPT_ITI.1-CSPP Inter-TSF detection of modification

Dependencies: None

FPT_ITI.1.1-CSPP The TSF shall provide the capability to detect modification of [**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]*] 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-CSPP The TSF shall provide the capability to verify the integrity of [**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.

Extension: See text in FPT_ITI.1.1 and FPT_ITI.1.2

FPT_ITT.1-CSPP Basic Internal TSF data transfer

Dependencies: None

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

Extension: See text in FPT_ITT.1.1

FPT_RCV.2 Automated recovery

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

FPT_RCV.2.1 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.

FPT_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.

FPT_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 each function within the TSC is allowed to proceed.

FPT_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.

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]*] when interpreting the TSF data from another trusted IT product.

Refinement - added element, clarifying intent:

FPT_TDC.1.3-CSPP The TSF shall support maintaining consistent 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.

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]*].

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)] and ***[PP selection:*** *periodically during normal operation]* and [***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

FPT_SYN-CSPP.1 TSF synchronization
Non-CC component

Extension:

Not hierarchical to any other component.

Dependencies: None

FPT_SYN-CSPP.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.

RESOURCE UTILIZATION (FRU)

FRU_RSA.1-CSPP Maximum quotas

Dependencies: None

FRU_RSA.1.1-CSPP The TSF shall enforce maximum quotas 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, subjects] can use *[**PP selection:** simultaneously, over a specified period of time]*.

TOE ACCESS (FTA)

FTA_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]*].

FTA_MCS.1-CSPP Basic limitation on multiple concurrent sessions

Dependencies: FIA_UID.1

FTA_MCS.1.1-CSPP The TSF shall [**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.

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

Refinement: See text in FTA_MCS.1.2
Extension: See text in FTA_MCS.1.1-CSPP

FTA_SSL.1 TSF initiated session locking

Dependencies: FIA_UAU.1

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

clearing or overwriting display devices, making the current contents unreadable;

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

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

FTA_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:

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

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].

FTA_SSL.3 TSF-initiated termination

Dependencies: None

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

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

FTA_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

FTA_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]*].

TRUSTED PATH/CHANNELS (FTP)

FTP_ITC.1-CSPP Inter-TSF trusted channel

Dependencies: None

FTP_ITC.1.1-CSPP 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 [**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 [**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]*].

Extension: See text in FTP_ITC.1.1-CSPP

FTP_TRP.1-CSPP Trusted path

Dependencies: None

FTP_TRP.1.1-CSPP 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 [**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 [**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,] [**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]*].

Extension: See text in FTP_TRP.1.1

APPENDIX C: ASSURANCE REQUIREMENT DETAILS

CONFIGURATION MANAGEMENT (ACM)

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.

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.

DELIVERY AND OPERATION (ADO)

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

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.

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.

DEVELOPMENT (ADV)

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.

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.

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.

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.

GUIDANCE DOCUMENTS (AGD)

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.

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.

LIFE CYCLE SUPPORT (ALC)

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.

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.

TESTS (ATE)

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.

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.

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.

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.

VULNERABILITY ASSESSMENT (AVA)

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.

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.

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.

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.

MAINTENANCE OF ASSURANCE (AMA)

None

APPENDIX D: IT-ENVIRONMENT FUNCTIONAL REQUIREMENT DETAILS

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 CSPP guidance document is the entire IT system, this section is currently empty. In a "compliant" CSPP PP, this section would provide detailed, CC requirements for the IT surrounding the TOE.

APPENDIX E: RATIONALE FOR CSPP PROTECTION PROFILE GUIDANCE

This appendix contains the rationale for the CSPP Protection Profile Guidance document. As PP rationale is frequently published as a separate document (to reduce the size of the base PP), the information in this appendix is formatted as though it were a separate document. This facilitates its use as a template for the rationale for a CSPP "compliant" PP.

TABLE OF CONTENTS

SECTION **PAGE**

TABLE OF TABLES

SECTION **PAGE**

1.0 INTRODUCTION

The purpose of this rationale document is to show that the CSPP protection profile (PP) guidance is internally consistent, accurate, and complete. This is accomplished by the individual rationales listed in Table 1-1.

Taken together, these rationale show (at the lower level of rigor appropriate for EAL-2 level evaluations) that PPs built using the CSPP list of functional and assurance requirements are suitable for describing a specific user need within the scope of those described in the CSPP introduction and TOE description.

Table 1-1 CSPP Rationale Overview

Nature of Rationale	Purpose	Section
Discuss the usage assumptions, showing that they are necessary and reasonable.	Show that the security environment description is consistent with the introduction and the TOE description.	2.1
Discuss the security policies, showing that they are necessary and reasonable.		2.2
Discuss the security threats, showing that they are necessary and reasonable.		2.3
Discuss the general assurance level, showing that it is appropriate.		2.4
Map security objectives to policy and threat	Show necessity of CSPP objectives	3.1
Map policy/threat to security objectives	Show completeness of CSPP objectives	3.2
Compare environmental security objectives with CSPP introduction and TOE description	Show correctness of CSPP objectives	3.3
Map functional requirement to dependencies and security objectives	Show necessity of CSPP functionality	4.1
Map security objectives to functional requirements and justify SOF claims	Show sufficiency of CSPP functionality	4.2
Map dependencies for CSPP functionality to CSPP requirement meeting that dependency	Show correctness of CSPP functionality	4.3.1
Discuss operations performed on CSPP function components (iteration, assignment, selection, or refinement)		4.3.2
Discuss functional operations deferred to ST		4.3.3
Discuss non-CC functional extensions		4.3.4

Nature of Rationale	Purpose	Section
Discuss basic assurance goals	Show necessity of CSPP assurances	5.1.1
Show EAL2 is the correct base level by mapping necessary components not in EAL2 to need and unnecessary components in EAL3 to rationale for being not needed.		5.1.2
Map EAL2 augmentation to need		5.1.3
Map unused CC components to reason for not being used	Show sufficiency of CSPP assurances	5.2
Map dependencies for CSPP assurance to CSPP requirement meeting that dependency	Show correctness of CSPP assurances	5.3.1
Discuss operations performed on CSPP assurance components (iteration, assignment, selection, or refinement)		5.3.2
Discuss assurance operations deferred to ST		5.3.3
Discuss non-CC assurance extensions		5.3.4

2.0 SECURITY ENVIRONMENT RATIONALE

2.1 USAGE ASSUMPTIONS

The intent of this rationale is to show that each of the CSPP usage assumptions is necessary and reasonable in light of the CSPP introduction and TOE description. This is accomplished in Table 2.1-1.

Table 2.1-1 Assumption Rationale

Name	Assumption	Rationale
A. ADMIN	The security features of the TOE are competently administered on an on-going basis.	Unless the system is administered competently in an on-going manner, security is not feasible. Therefore this assumption is both necessary and reasonable.
A.COTS	The TOE is constructed from near-term achievable, commercial off the shelf information technology.	This assumption represents the key design constraint used in the development of CSPP.
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.	The assurance level that can be reasonably expected for near-term achievable COTS does not support resistance to sophisticated attacks.
A.USER-NEED	Authenticated users recognize the need for a secure IT environment.	Unless the users internalize a need for security they are bound to circumvent it. This fact is commonly recognized and a primary driver in security awareness training that is common place both in government and industry. Therefore this assumption is both necessary and reasonable.
A.USER-TRUST	Authenticated users are generally trusted to perform discretionary actions in accordance with security policies.	The authenticated users are trusted in this manner in most organizations. With CSPP compliant systems, the users have a fair amount of discretion and must be trusted to handle it appropriately. Therefore this assumption is both necessary and reasonable.

2.2 SECURITY POLICIES

Table 2.2-1 presents the rationale showing that each of the CSPP security policies is both necessary and reasonable.

Table 2.2-1 Security Policy Rationale

Name	Policy	Rationale
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.	It is an essential premise for CSPP systems that the access to objects is controlled. The nature of this control is clearly that characteristics of the proposed access (entity, type of access; e.g., read, write, and nature of access; e.g., local, remote, time-of-day) are compared with attributes of the object to determine whether the access to be allowed. This policy is both necessary and reasonable.
P.ACCOUNT	Users must be held accountable for security-relevant actions.	It is generally considered standard, best practice to hold users accountable for their actions. This policy is necessary and reasonable.
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.	This policy is necessary and reasonable.
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.	As IT becomes a central part of the business or mission process, the potential impact on the organization, and personally on the organization's senior management, has dramatically increased. With this is coming the recognition that due care and diligence with respect to computing security is now as important as the organization's fiduciary responsibilities in other areas. The policy is necessary and reasonable.
P.INFO-FLOW	Information flow between IT components must be in accordance with established information flow policies.	As generic guidance, CSPP must cover a wide-range of situations. This will include organizations with policy mandating information flow control. If there is no such policy in a specific installation, then PPs targeted against such situations will be so written. But in the general case, this policy is necessary and reasonable.
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.	It is standard practice to identify and authenticate users. It has also become common to allow anonymous access in cases such as a public web server. This policy is necessary and reasonable.

Name	Policy	Rationale
P.NETWORK	The organization's IT security policy must be maintained in the environment of distributed systems interconnected via insecure networking.	Distributed information systems is a fact that CSPP must incorporate. This policy is necessary and reasonable.
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.	Physical protection is a common element of organizational policies and clearly necessary. This policy is necessary and reasonable.
P.SURVIVE	The IT system, in conjunction with its environment, must be resilient to insecurity, resisting the insecurity and/or providing the means to detect an insecurity and recover from it.	Since IT has become an essential component of many mission/business processes, this is a key element of a successful computing security program. This is also becoming widely understood as such. This policy is necessary and reasonable.
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.	Organizations generally accept this as a need and are implementing it. Unless the users are able to make appropriate choices, they are likely to defeat the security controls. This policy is necessary and reasonable.
P.USAGE	The organization's IT resources must be used for only for authorized purposes.	With recent hacking to use corporate and government resources for a number of unauthorized activities like spamming, software piracy, and breaking other systems, this policy is being even more vigorously pursued. Yet "Authorized-only use" has been a recognized portion of IT policy for decades. This policy is necessary and reasonable.

2.3 THREATS TO SECURITY

For each threat to be covered by CSPP, Table 2.3-1 gives a rationale for that threat, explaining why, if not met by the TOE, it is appropriate to be classed as environment or joint.

Table 2.3-1 Security Threat Rationale

Name	Threat	Rationale
Environment: T.ACCESS-NON-TECHNICAL	An authenticated user may gain non-malicious, unauthorized access using non-technical means.	Like T-ENTRY-NON-TECHNICAL above, this threat is explicitly non-technical and its mitigation requires environmental controls. T.ACCESS-NON-TECHNICAL is listed as a separate threat from T.ENTRY-NON-TECHNICAL because the likely mitigating controls applied to authenticated users are different from those applied to individuals not authorized IT access.
Environment: 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.	Users are generally trusted to do the right thing (A.USER-TRUST). However, they will make mistakes and it is likely that situations will occur where users circumvent security "to get the job done", out of curiosity, or for the sake of the challenge to do so. This threat is listed to derive objectives for the IT other than the TOE that can reasonably be met with COTS.
Environment: 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.	Because CSPP is not intended to be able to resist all attacks, detection and response are critical. T.AUDIT-CONFIDENTIALITY-Non-TOE is highlighted as a contributor toward a potential failure in the detection and response capability in IT other than the TOE.
Environment: 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.	Because CSPP is not intended to be able to resist all attacks, detection and response are critical. T.AUDIT-CORRUPTED-Non-TOE is highlighted as a significant contributor toward a potential failure in the detection and response capability of IT other than the TOE.
Environment: T.DENIAL-Non-TOE	The IT (other than the TOE) may be subjected to an unsophisticated, denial-of-service attack.	In the real-world, CSPP systems will be subjected to denial of service and meeting P.SURVIVE requires addressing this threat to IT other than the TOE. CSPP technical controls are limited to addressing this threat, in lieu of the threat of sophisticated attacks, because CSPP is a baseline for COTS that is near-term achievable. Protecting against the greater risk from sophisticated actions is beyond the scope of COTS expectations.

Name	Threat	Rationale
Environment: T.DENIAL-SOPHISTICATED	The system may be subjected to a sophisticated, denial-of-service attack.	COTS IT is not expected to resist sophisticated attacks and must therefore, rely on protections provided by its environment to maintain availability in the face of such threats.
Environment: T.ENTRY-NON-TECHNICAL	An individual, other than an authenticated user, may gain access to processing resources or information using non-technical means.	This threat is explicitly non-technical and beyond the scope of CSPP technical controls. This necessitates environmental controls.
Environment: 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.	CSPP technical controls are limited to addressing this threat to IT other than the TOE, in lieu of the threat of sophisticated attacks, because CSPP is a baseline for COTS that is near-term achievable. Protecting against the greater risk from sophisticated actions is beyond the scope of COTS expectations.
Environment: T.ENTRY-SOPHISTICATED	An individual, other than an authenticated user, may gain access to processing resources or information using a sophisticated, technical attack.	COTS IT is not expected to protect against sophisticated, technical attacks. There is no reasonable expectation that compliant IT will significantly increase the work-factor required to accomplish a successful, high-grade attack, over that associated with a non-compliant IT. Therefore, this threat is largely addressed by the TOE environment.
Environment: 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.	IT must not misrepresent what is within the scope of their security mechanisms to correctly interpret. The man-machine interface, at least with respect to the basic security state of the system, must be free from obvious errors that might lead an responsible, competent individual to misunderstand the system's security state.
Environment: T.PHYSICAL	Security-critical parts of the system may be subjected to a physical attack that may compromise security.	As explained in the discussion concerning A.PHYSICAL the physical protection of IT resources is critical. Since CSPP is a baseline for near-term COTS, it is not reasonable to expect IT mechanisms that address physical security to any significant degree.
Environment: T.RECORD-EVENT-Non-TOE	Security relevant events not under control of the TOE may not be recorded.	Because CSPP is not intended to be able to resist all attacks, detection and response are critical. T.RECORD-EVENT-Non-TOE is highlighted as a significant contributor toward a potential failure in the detection and response capability in IT other than the TOE.

Name	Threat	Rationale
Environment: 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.	CSPP represents, in general, multi-user or multi-process systems. As such, mechanisms addressing this threat are clearly needed and also common place. In the general case, some resource control will be outside the scope of the TOE and must be addressed by the environment.
Environment: 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.	Because CSPP is not intended to be able to resist all attacks, detection and response are critical. T.TRACEABLE-Non-TOE is highlighted as a significant contributor toward a potential failure in the detection and response capability in IT other than the TOE.
TOE: 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.	Users are generally trusted to do the right thing (A.USER-TRUST). However, they will make mistakes and it is likely that situations will occur where users circumvent security "to get the job done", out of curiosity, or for the sake of the challenge to do so. CSPP technical controls are limited to addressing this threat, in lieu of the threat of malicious user actions, because CSPP is a baseline for COTS that is near-term achievable. Protecting against the greater risk from malicious actions is beyond the scope of COTS expectations.
TOE: T.AUDIT-CONFIDENTIALITY-TOE	For audit trails under control of the TOE, records of security events may be disclosed to unauthorized individuals or processes.	Because CSPP is not intended to be able to resist all attacks, detection and response are critical. T.AUDIT-CONFIDENTIALITY-TOE is highlighted as a contributor toward a potential failure in the detection and response capability in the TOE.
TOE: T.AUDIT-CORRUPTED-TOE	For audit trails under control of the TOE, records of security events may be subjected to unauthorized modification or destruction.	Because CSPP is not intended to be able to resist all attacks, detection and response are critical. T.AUDIT-CORRUPTED-TOE is highlighted as a significant contributor toward a potential failure in the detection and response capability in the TOE.
TOE: T.CRASH-TOE	The secure state of the TOE could be compromised in the event of a system crash.	Systems crash and secure systems may crash into an insecure state. Mitigating against this is reasonable, prudent, and within the scope of CSPP technical controls.
TOE: T.DENIAL-TOE	The TOE may be subjected to an unsophisticated, denial-of-service attack.	In the real-world, CSPP systems will be subjected to denial of service. This fact and the need to meet P.SURVIVE require addressing this threat. CSPP technical controls are limited to addressing this threat, in lieu of the threat of sophisticated attacks, because CSPP is a baseline for COTS that is near-term achievable. Protecting against the greater risk from sophisticated actions is beyond the scope of COTS expectations.

Name	Threat	Rationale
TOE: 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.	CSPP technical controls are limited to addressing this threat, in lieu of the threat of sophisticated attacks, because CSPP is a baseline for COTS that is near-term achievable. Protecting against the greater risk from sophisticated actions is beyond the scope of COTS expectations.
TOE: 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.	The TOE must not misrepresent what is within the scope of their security mechanisms to correctly interpret. The man-machine interface, at least with respect to the basic security state of the system, must be free from obvious errors that might lead an responsible, competent individual to misunderstand the system's security state.
TOE: T.RECORD-EVENT-TOE	Security relevant events controlled by the TOE may not be recorded.	Because CSPP is not intended to be able to resist all attacks, detection and response are critical. T.RECORD-EVENT-TOE is highlighted as a significant contributor toward a potential failure in the detection and response capability in the TOE.
TOE: T.RESOURCES-TOE	The shared, internal TOE resources may become exhausted due to system error or non-malicious user actions.	CSPP represents, in general, multi-user or multi-process systems. As such, mechanisms addressing this threat are clearly needed and also common place.
TOE: 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 penetrations by either lower-grade attacks may result is an intentionally corrupted system state. A CSPP compliant TOE is expected to adequately mitigate against such corruption. (Threats due to high-grade attacks are covered by T.SYSEM-CORRUPTED.)
TOE: T.TRACEABLE-TOE	Security relevant events controlled by the TOE may not be traceable to the user or system process associated with the event.	Because CSPP is not intended to be able to resist all attacks, detection and response are critical. T.TRACEABLE-TOE is highlighted as a significant contributor toward a potential failure in the detection and response capability in the TOE.
Joint: T.ACCESS-MALICIOUS	An authenticated user may obtain unauthorized access for malicious purposes.	The TOE mechanisms for controlling access will help address this threat. But since CSPP is a baseline for near-term COTS, this mitigation is not likely to be sufficient for the risks implied by this threat. Hence additional, environmental controls are essential. A compliant solution may provide for some trade-off between environment and TOE in meeting this threat.

Name	Threat	Rationale
Joint: 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.	Humans make mistakes, and if that human is the system administrator then the security consequences may be great. The TOE is expected to provide some mitigation, but, especially since CSPP is a baseline for near-term COTS, the TOE controls are not expected to be adequate. Environmental controls are needed as well. A compliant solution may provide for some trade-off between environment and TOE in meeting this threat.
Joint: T.CRASH-SYSTEM	The secure state of the system could be compromised in the event of a system crash.	Systems crash and secure systems may crash into an insecure state. Depending on the specifics of a given TOE, it may well contribute to system recovery, in addition to its own. IT other than the TOE is likely to have a significant responsibility. Non-IT environmental controls will likely be needed as well. A compliant solution may provide for some trade-off between environment and TOE in meeting this threat.
Joint: T.INSTALL	The TOE may be delivered or installed in a manner that undermines security.	The TOE can be expected to help address this threat, but significant environmental controls are also expected. There is the distinct potential for trade-offs between environment and TOE in meeting this threat, while maintaining consistency with the intent and constraints of this PP.
Joint: T.OPERATE	Security failures may occur because of improper operation of the TOE; e.g., the abuse of authorized privileges.	While the TOE can be expected to provide mechanisms that help cover this threat, full coverage inherently includes actions that must be addressed by environmental controls. A compliant solution may provide for some trade-off between environment and TOE in meeting this threat.
Joint: T.SYSTEM-CORRUPTED	The security state of the system, as a result of another threat, may be intentionally corrupted to enable future insecurities.	System penetrations by either sophisticated attackers or attackers using sophisticated tools will likely result is an intentionally corrupted system state. COTS IT is not expected to adequately mitigate against such corruption. The IT mechanisms are expected, in concert with environmental controls, to support detection of such corruption. A compliant solution may provide for some trade-off between environment and TOE in meeting this threat.

2.4 GENERAL ASSURANCE LEVEL

The rationale for the general level of assurance for CSPP is fully covered in sections 5.1.1 “Basic Assurance Goals” and 5.1.2 “EAL Selection”.

3.0 SECURITY OBJECTIVES RATIONALE

The rationale for the set of CSPP security objectives will be based upon the following:

Necessity – all required. Each objective must contribute to satisfying a security policy or countering a threat.

Complete – satisfy all policies and counter all threats. The list of security objectives must satisfy the policies and adequately counter the threats listed in CSPP.

Correct –

TOE verses environment. The allocation of policy enforcement and threat mitigation to the environment must be reasonable.

Correct statement. The security objective must correctly state its intent.

3.1 NECESSARY OBJECTIVES

Tables 3.1-1, 3.1-2, and 3.1-3 show the mapping of security objectives to threats and policies. This table indicates that each objective contributes to countering a threat or satisfying a policy. Thus there are no unnecessary objectives.

Table 3.1-1 Necessary Objectives – Mapping Environmental Objectives to Policy and Threat

Environmental Security Objective	Threat or Policy
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 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.	P.ACCESS
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.	T.ACCESS-Non-TOE

NOTE: This objective is limited to 'non-malicious' because IT controls in the notional CSPP system are not expected to provide sufficient mitigation for the greater negative impact that 'malicious' implies.	
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: The shared, internal resources of IT other than the TOE may become exhausted due to system error or non-malicious user actions.	P.SURVIVE T.RESOURCES-Non-TOE

Table 3.1-2 Necessary Objectives –
Mapping TOE Objectives to Policy and Threat

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, 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 CSPP controls are not expected to be sufficient mitigation for the greater negative impact that 'malicious' implies.	T.ACCESS-TOE
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.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.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.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	T.OBSERVE-TOE

possible failure modes, is to be achieved with a moderate, verses high, degree of effectiveness.	
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

Table 3.1-3 Necessary Objectives –
Mapping Joint Objectives to Policy and Threat

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, but the majority of the focus will be on detection and response, with high effectiveness for specified failures. For general failure, this will be accomplished with low effectiveness.	P.SURVIVE T.CRASH-SYSTEM

3.2 COMPLETE OBJECTIVES

Tables 3.2-1 and 3.2-2 show that all policies and threats are covered by security objectives. While this alone does not prove completeness, a simple mapping is considered sufficient in light of the general level of assurance provided by EAL2.

Table 3.2-1 Complete Objectives – Mapping Policy to Objectives

Policy	Objectives
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.	O.ACCESS-NON-TOE O.ACCESS-TOE O.AUTHORIZE-NON-TOE O.AUTHORIZE-TOE
P.ACCOUNT Users must be held accountable for security-relevant actions.	O.ACCOUNT-NON-TOE O.ACCOUNT-TOE
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.	O.COMPLY
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.	O.DUE-CARE
P.INFO-FLOW Information flow between IT components must be in accordance with established information flow policies.	O.INFO-FLOW
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.	O.KNOWN-NON-TOE O.KNOWN-TOE
P.NETWORK The organization's IT security policy must be maintained in the environment of distributed systems interconnected via insecure networking.	O.NETWORK
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.	O.PHYSICAL
P.SURVIVE The IT system, in conjunction with its environment, must be resilient to insecurity, resisting the insecurity and/or providing the means to detect an insecurity and recover from it.	O.AVAILABLE-NON-TOE O.AVAILABLE-TOE O.DENIAL-SOPHISTICATED O.DETECT-SYSTEM O.DETECT-TOE O.DETECT-SOPHISTICATED O.RECOVER-SYSTEM O.RECOVER-TOE O.RESOURCES-TOE
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.	O.OPERATE

Policy	Objectives
P.USAGE The organization's IT resources must be used for only for authorized purposes.	O.ENTRY-NON-TOE O.ENTRY-TOE

Table 3.2-2 Complete Objectives – Mapping Threats to Objectives

Threat	Objectives
T.ACCESS-MALICIOUS An authenticated user may obtain unauthorized access for malicious purposes.	O.ACCESS-MALICIOUS
T.ACCESS-NON-TECHNICAL An authenticated user may gain non-malicious, unauthorized access using non-technical means.	O.ACCESS-NON-TECHNICAL
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.	O.BYPASS-NON-TOE
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.	O.BYPASS-TOE
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.	O.MANAGE
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.	O.ACCOUNT-NON-TOE
T.AUDIT-CONFIDENTIALITY-TOE For audit trails under control of the TOE, records of security events may be disclosed to unauthorized individuals or processes.	O.ACCOUNT-TOE
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.	O.ACCOUNT-NON-TOE
T.AUDIT-CORRUPTED-TOE For audit trails under control of the TOE, records of security events may be subjected to unauthorized modification or destruction.	O.ACCOUNT-TOE
T.CRASH-SYSTEM The secure state of the system could be compromised in the event of a system crash.	O.RECOVER-SYSTEM
T.CRASH-TOE The secure state of the TOE could be compromised in the event of a system crash.	O,RECOVER-TOE
T.DENIAL-Non-TOE The IT (other than the TOE) may be subjected to an unsophisticated, denial-of-service attack.	O.AVAILABLE-NON-TOE
T.DENIAL-SOPHISTICATED The system may be subjected to a sophisticated, denial-of-service attack.	O.DENIAL-SOPHISTICATED
T.DENIAL-TOE The TOE may be subjected to an unsophisticated, denial-of-service attack.	O.AVIALABLE-TOE

T.ENTRY-NON-TECHNICAL An individual, other than an authenticated user, may gain access to processing resources or information using non-technical means.	O.ENTRY-NON-TECHNICAL
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.	O.ENTRY-NON-TOE
T.ENTRY-SOPHISTICATED An individual, other than an authenticated user, may gain access to processing resources or information using a sophisticated, technical attack.	O.ENTRY-SOPHISTICATED
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.	O.ENTRY-TOE
T.INSTALL The TOE may be delivered or installed in a manner that undermines security.	O.OPERATE
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.	O.OBSERVE-NON-TOE
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.	O.OBSERVE-TOE
T.OPERATE Security failures may occur because of improper operation of the TOE; e.g., the abuse of authorized privileges.	O.OPERATE
T.PHYSICAL Security-critical parts of the system may be subjected to a physical attack that may compromise security.	O.PHYSICAL
T.RECORD-EVENT-Non-TOE Security relevant events not under control of the TOE may not be recorded.	O.ACCOUNT-NON-TOE
T.RECORD-EVENT-TOE Security relevant events controlled by the TOE may not be recorded.	O.ACCOUNT-TOE
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.	O.RESOURCES-NON-TOE
T.RESOURCES-TOE The shared, internal TOE resources may become exhausted due to system error or non-malicious user actions.	O.RESOURCES-TOE
T.SYSTEM-CORRUPTED The security state of the system, as a result of another threat, may be intentionally corrupted to enable future insecurities.	O.DETECT-SOPHISTICATED O.DETECT-SYSTEM

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.	O.DETECT-TOE
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.	O.ACCOUNT-NON-TOE
T.TRACEABLE-TOE Security relevant events controlled by the TOE may not be traceable to the user or system process associated with the event.	O.ACCOUNT-TOE

3.3 CORRECT OBJECTIVES

Tables 3.3-1, 3.3-2, and 3.3-3 provide a rationale for the correctness of each of security objectives. Where there is a one-to-one match between a policy or threat, that policy or threat is the rationale. For the environmental and joint objectives, an explanation is provided for not including the objective in the list of TOE security objectives.

Table 3.3-1 Correct Objectives - Mapping Environmental Security Objective to Rationale

Environmental Security Objective	Rationale
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 The countermeasures necessary to deal with this threat are inherently environmental. The objectives for protecting against non-technical access and non-technical entry are listed separately due to the potential for differing types of countermeasures. The measures used to address improper access by authorized personnel are not necessarily the same as those imposed to deal with actions by unauthorized individuals.
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 and generic CSPP need for the capability for public access. This is an environmental objective because the TOE will not be able to enforce access control to IT resources outside of its control. O.ACCESS-TOE is the companion TOE objective.
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 This is an environmental objective because the TOE is unable to ensure accountability for actions not under its control. O.ACCOUNT-TOE is the companion TOE objective.
O.AUTHORIZE-Non-TOE: The IT other than 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 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.	This objective is implied by P.ACCESS. In order to provide access to "authorized" users, there must be a means of authorizing. This is an environmental objective because the TOE is unable to manage authorizations for resources not under its control. O.AUTHORIZE-TOE is the companion TOE objective.

Environmental Security Objective	Rationale
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, in light of real-world attacks, makes dealing with denial-of-service essential. The basic cost/benefit tradeoffs inherent in CSPP necessitate calling out only the less sophisticated of such attacks. This is an environmental objective because the TOE is unable to ensure availability of IT not under its control. O.AVAILABLE-TOE is the companion TOE objective.
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 CSPP system are not expected to provide sufficient mitigation for the greater negative impact that 'malicious' implies.	This objective is called out to distinguish between the higher risk of purposeful, malicious actions (for which IT technical measures from COTS products are not expected to be adequate) and the lower risk of either unintended or non-malicious actions. This is an environmental objective because the TOE cannot address enforcement within IT not under its control. O.BYPASS-TOE is the companion TOE objective.
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.	T.DENIAL-SOPHISTICATED COTS IT is not expected to provide mechanisms that effectively deal with this threat. Effectively dealing with real-world threat-agents requires the countermeasures provided by the TOE environment.
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 See rationale for T.DENIAL-SOPHISTICATED.
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 See rationale for T.ACCESS-NON-TECHNICAL.

Environmental Security Objective	Rationale
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.	T.ENTRY The basic cost/benefit tradeoffs inherent in CSPP necessitate calling out only the less sophisticated of attacks. This is an environmental objective because the TOE is not able to prevent unauthorized entry to IT not under its control. T.ENTRY-TOE is the companion TOE objective.
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 See rationale for T.DENIAL-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 This is an environmental objective because the TOE is unable to trace actions not under its control. O.KNOWN-TOE is the companion TOE objective.
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 This is an environmental objective because the TOE is unable to impact what is presented by IT not under its control. T.OBSERVE-TOE is the companion TOE objective.
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.	P.PHYSICAL (and also T.PHYSICAL) CSPP is intended for near-term, COTS. As such, it is not reasonable to expect physical security countermeasures within the TOE itself. Therefore physical security is an environmental objective.
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.	T.RESOURCES-NON-TOE The TOE cannot ensure the availability of resources not under its control. Therefore this is an environmental objective. O.RESOURCES-TOE is the companion TOE objective.

Table 3.3-2 Correct Objectives -
Mapping TOE Security Objective to Rationale

TOE Security Objective	Rationale
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 and generic CSPP need for the capability for public access. O.ACCESS-NON-TOE is the companion environmental objective.
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 O.ACCESSS-NON-TOE is the companion environmental objective.
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.	This objective is implied by P.ACCESS. In order to provide access to "authorized" users, there must be a means of authorizing. O.AUTHORIZE-NON-TOE is the companion environmental objective.
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, in light of real-world attacks, makes dealing with denial-of-service essential. The basic cost/benefit tradeoffs inherent in CSPP necessitate calling out only the less sophisticated of such attacks. O.AVAILABLE-NON-TOE is the companion environmental objective.
O.BYPASS-TOE: The TOE must prevent errant or non-malicious, 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 CSPP controls are not expected to be sufficient mitigation for the greater negative impact that 'malicious' implies.	This objective is called out to distinguish between the higher risk of purposeful, malicious actions (for which the TOE technical measures are not expected to be adequate) and the lower risk of either unintended or non-malicious actions. O.BYPASS-NON-TOE is the companion environmental objective.

TOE Security Objective	Rationale
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.	This is an essential counterpart to O.RECOVER-TOE in accomplishing P.SURVIVE.
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.	T.ENTRY O.ENTRY-NON-TOE is the companion environmental objective.
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.KNOWN-NON-TOE is the companion environmental objective.
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 O.OBSERVE-NON-TOE is the companion environmental objective.
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 is the major driver for this objective. CSPP must provide an effective cost/benefit tradeoff for technical security countermeasures. This being the case, detection and recovery is a practical alternative to trying to prevent insecurity for many classes of potential problems. Also, insecurity is bound to happen and recovery is essential in order for the system capability to survive.
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.	T.RESOURCES-TOE O.RESOURCES-NON-TOE is the companion environmental objective.

Table 3.3-2 Correct Objectives -
Mapping Joint Security Objective to Rationale

Joint Security Objective	Rationale
O.ACCESS-MALICIOUS The TOE environment must sufficiently mitigate the threat of malicious actions by authenticated users.	T.ACCESS-MALICIOUS The TOE may provide mechanisms that seek to deal with this threat. However, the general level of assurance for CSPP is not sufficient to rely on these mechanisms. Effectively dealing with real-world threat-agents requires the addition of countermeasures provided by the TOE environment.
O.COMPLY The TOE environment, in conjunction with controls implemented by the TOE, must support full compliance with applicable laws, regulations, and contractual agreements.	P.COMPLY Complying with policy will require more than can be accomplished with the TOE itself. The TOE environment must also supply countermeasures to ensure policy compliance.
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.	T.SYSTEM-CORRUPTED, P.SURVIVE The TOE may be able to support this activity for other IT in the system, hence it is not strictly an environmental objective. However, the TOE is unlikely to be able to accomplish the entire task, having to operate in conjunction with mechanisms in other IT - hence not strictly a TOE objective.
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.	P.DUE-CARE The TOEs of CSPP compliant PPs can be expected to directly support this policy, but can not be expected to have sufficient internal countermeasures to meet this policy. Environmental controls will be an important part of demonstrating due-care and diligence.
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 The TOE may well play a major role in enforcement of information flow controls, but it is likely that other IT and non-IT controls will be required to meet this policy.
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.	T.ADMIN-ERROR This is an environmental objective because the actions required include, to a large degree, non-technical countermeasures. The TOE is expected to support, however, by providing mechanisms and interfaces that ease the burden of ensuring correct delivery, installation, and operation.

Joint Security Objective	Rationale
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.	T.INSTALL, T.OPERATE, T.ADMIN-ERROR See rationale for O.MANAGE.
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, but the majority of the focus will be on detection and response, with high effectiveness for specified failures. For general failure, this will be accomplished with low effectiveness.	P.SURVIVE, T.CRASH-SYSTEM The TOE may well contribute directly to overall system recovery - hence not strictly an environmental objective. But the TOE is not likely to be able to accomplish system recovery without direct involvement by other IT and the application of non-IT controls - hence not strictly a TOE objective.

4.0 TOE FUNCTIONAL REQUIREMENTS RATIONALE

The rationale for the set of CSPP functions will be based upon the following:

Necessary – all required. Each function either (1) meets a dependency for a necessary functional or assurance requirement or (2) is required in order to meet one or more security objectives.

Sufficient – meet objectives. The list of functions completely meets the IT security objectives and the TOE's responsibilities with respect to environmental objectives. Also, the strength of function claims are appropriate for the stated effectiveness claims.

Correct –

Cover dependencies. All dependencies for each functional requirement are satisfied.

Operations correct. All operations on CC elements are justified and have been performed in accordance with CC guidelines and in accordance with intended CSPP purpose.

Deferred operations correct. All deferred operations are justified.

Extensions correct. All extensions to CC elements and components are justified and have been performed in accordance with CC guidelines and in accordance with intended CSPP purpose.

4.1 NECESSARY TOE FUNCTIONALITY

Table 4.1-1 provides the rationale for the necessity of each TOE functional requirement included in CSPP. Necessity is demonstrated if, for each functional requirement, there is at least one security objective that cannot be met without it. This can be achieved either by directly addressing one or more objectives or by meeting a required dependency for another functional component that directly addresses security objectives. The latter case is true for functional requirements number 3 and 37.

Table 4.1-1 Necessary Functionality – Mapping Function to Requirement

#	Functional Component	Name	Dependency for	Required to help address
1	FAU_GEN.1-CSPP	Audit data Generation	FAU_GEN.2 FAU_SAR.1 FAU_SEL.1 FAU_STG.1	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		O.ACCOUNT-TOE
3	FAU_SAR.1	Audit Review	FAU_SAR.2 FAU_SAR.3	
4	FAU_SAR.2	Restricted Audit Review		O.BYPASS-TOE
5	FAU_SAR.3	Selectable Audit Review		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-CSPP	Selective Audit		O.DUE-CARE O.DETECT-TOE O.DETECT-SYSTEM O.MANAGE O.OPERATE O.COMPLY

#	Functional Component	Name	Dependency for	Required to help address
7	FAU_STG.1	Protected audit trail storage	FAU_STG.3	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		O.ACCOUNT-TOE O.DUE-CARE O.MANAGE
9	FDP_ACC.1	Subset Access Control	FDP_ACF.1 FDP_ETC.1 FDP_ITC.1 FDP_ITT.1 FDP_UCT.1 FDP_UIT.1 FMT_MSA.1	O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.DUE-CARE O.COMPLY O.AVAILABLE-TOE O.RESOURCES-TOE
10	FDP_ACF.1-CSPP	Security Attribute Based Access Control	FDP_ACC.1	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		O.BYPASS-TOE O.DUE-CARE O.ENTRY-TOE O.AVAILABLE-TOE
12	FDP_ETC.1-CSPP	Export of user data without security attributes		O.BYPASS-TOE O.DUE-CARE O.ENTRY-TOE O.AVAILABLE-TOE
13	FDP_IFC.1	Subset information flow control	FDP_ETC.1 FDP_IFF.1 FDP_IFF.8 FDP_ITC.1 FDP_ITT.1 FDP_UCT.1 FDP_UIT.1 FMT_MSA.1	

#	Functional Component	Name	Dependency for	Required to help address
14	FDP_IFF.1	Simple security attributes	FDP_IFC.1	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-TOE O.DUE-CARE
18	FDP_SDI.1	Stored data integrity monitoring		O.DETECT-TOE O.DETECT-SYSTEM O.RECOVER-TOE 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-TOE O.DETECT-SYSTEM O.ENTRY-TOE O.BYPASS-TOE O.DUE-CARE O.COMPLY
22	FIA_ATD.1	User Attribute Definition	FIA_USB.1	O.AUTHORIZE-TOE
23	FIA_SOS.1	Verification of Secrets		O.BYPASS-TOE O.DUE-CARE O.COMPLY
24	FIA_SOS.2	TSF Generation of Secrets		O.BYPASS-TOE O.DUE-CARE O.COMPLY
25	FIA_UAU.1	Timing of authentication	FIA_AFL.1 FIA_UAU.7 FTA_SSL.1 FTA_SSL.2	O.KNOWN-TOE
26	FIA_UAU.5	Multiple authentication mechanisms		O.NETWORK
27	FIA_UAU.6	Re-authenticating		O.BYPASS-TOE
28	FIA_UAU.7	Protected authentication feedback		O.BYPASS-TOE
29	FIA_UID.1	Timing of identification	FAU_GEN.2 FIA_UAU.1 FMT_SMR.1 FTA_MCS.1	O.KNOWN-TOE

#	Functional Component	Name	Dependency for	Required to help address
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		O.MANAGE O.DUE-CARE
32	FMT_MSA.1	Management of security attributes	FMT_MSA.3	O.MANAGE O.DUE-CARE O.AUTHORIZE-TOE
33	FMT_MSA.3	Static attribute initialization	FDP_ACF.1 FDP_IFF.1 FDP_IFF.8 FDP_ITC.1	O.MANAGE O.DUE-CARE O.AUTHORIZE-TOE
34	FMT_MTD.1	Management of TSF data	FAU_SEL.1	O.MANAGE O.DUE-CARE
35	FMT_SAE.1	Time-Limited Authorization		O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.AUTHORIZE-TOE O.MANAGE O.DUE-CARE
36	FMT_SMR.1	Security roles	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_SAE.1	O.MANAGE O.DUE-CARE
37	FPT_AMT.1	Abstract Machine Testing	FPT.TST.1	
38	FPT_FLS.1	Failure with preservation of secure state		O.RECOVER-TOE O.RECOVER-SYSTEM
39	FPT_ITC.1-CSPP	Inter-TSF Confidentiality During Transmission		O.NETWORK
40	FPT_ITI.1-CSPP	Inter-TSF detection of modification		O.NETWORK
41	FPT_ITT.1-CSPP	Basic internal TSF data transfer protection	FPT_TRC.1	O.NETWORK
42	FPT_RCV.2	Automated Recovery		O.RECOVER-TOE O.RECOVER-SYSTEM
43	FPT_RPL.1	Replay detection		O.NETWORK

#	Functional Component	Name	Dependency for	Required to help address
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		O.NETWORK
47	FPT_TRC.1	Internal TSF consistency		O.NETWORK
48	FPT_TST.1	TSF Testing	FPT_RCV.2	O.DETECT-TOE O.DETECT-SYSTEM O.DUE-CARE
49	FRU_RSA.1-CSPP	Maximum quotas		O.RESOURCES-TOE
50	FTA_LSA.1	Limitation on scope of selectable attributes		O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.DUE-CARE
51	FTA_MCS.1-CSPP	Basic limitation on multiple concurrent session		O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.DUE-CARE
52	FTA_SSL.1	TSF-initiated session locking		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		O.BYPASS-TOE O.DUE-CARE
55	FTA_TAB.1-CSPP	Default TOE access banners		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		O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE

#	Functional Component	Name	Dependency for	Required to help address
58	FTP_ITC.1-CSPP	Inter-TSF trusted channel	FDP_UCT.1 FDP_UIT.1	O.NETWORK
59	FTP_TRP.1-CSPP	Trusted path	FDP_UCT.1 FDP_UIT.1	O.NETWORK
60	Non-CC FPT_SYN-CSPP.1	TSF synchronization FPT_STM.1 changed to be synchronization requirements (instead of just requiring a mechanism that supports it)	FPT_GEN.1 FMT_SAE.1	O.NETWORK

4.2 SUFFICIENT TOE FUNCTIONALITY

4.3 Coverage of Security Objectives

Tables 4.2-1 and 4.2-2 show completeness of the TOE functional set with respect to covering TOE and joint security objectives.

Table 4.2-1 Complete Functionality - Mapping TOE Security Objective to TOE Functionality

Security Objective	TOE Functionality
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.	9 FDP_ACC.1 10 FDP_ACF.1 30 FIA_USB.1 35 FMT_SAE.1 50 FTA_LSA.1 51 FTA_MCS.1 57 FTA_TSE.1
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.	1 FAU_GEN.1 2 FAU_GEN.2 5 FAU_SAR.3 7 FAU_STG.1 8 FAU_STG.3 55 FTA_TAB.1
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.	22 FIA_ATD.1 32 FMT_MSA.1 33 FMT_MSA.3 35 FMT_SAE.1
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.	9 FDP_ACC.1 10 FDP_ACF.1 11 FDP_DAU.1 12 FDP_ETC.1

Security Objective	TOE Functionality
O.BYPASS-TOE: The TOE must prevent errant or non-malicious, 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 CSPP controls are not expected to be sufficient mitigation for the greater negative impact that 'malicious' implies.	4 FAU_SAR.2 7 FAU_STG.1 11 FDP_DAU.1 12 FDP_ETC.1 17 FDP_RIP.1 21 FIA_AFL.1 23 FIA_SOS.1 24 FIA_SOS.2 27 FIA_UAU.6 28 FIA_UAU.7 30 FIA_USB.1 44 FPT_RVM.1 45 FPT_SEP.1 52 FTA_SSL.1 53 FTA_SSL.2 54 FTA_SSL.3 56 FTA_TAH.1
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.	1 FAU_GEN.1 5 FAU_SAR.3 6 FAU_SEL.1 7 FAU_STG.1 19 FDP_SDI.1 21 FIA_AFL.1 48 FPT_TST.1
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.	9 FDP_ACC.1 10 FDP_ACF.1 11 FDP_DAU.1 12 FDP_ETC.1 21 FIA_AFL.1 35 FMT_SAE.1 50 FTA_LSA.1 51 FTA_MCS.1 55 FTA_TAB.1 56 FTA_TAH.1 57 FTA_TSE.1
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.	25 FIA_UAU.1 29 FIA_UID.1
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.	56 FTA_TAH.1

Security Objective	TOE Functionality
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.	1 FAU_GEN.1 5 FAU_SAR.3 19 FDP_SDI.1 38 FPT_FLS.1 42 FPT.RCV.1
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.	9 FDP_ACC.1 10 FDP_ACF.1 49 FRU_RSA.1

Table 4.2-1 Complete Functionality -
Mapping Joint Security Objective to TOE Functionality

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.	1 FAU_GEN.1-CSPP 2 FAU_GEN.2 3 FAU_SAR.1 5 FAU_SAR.3 7 FAU_STG.1 9 FDP_ACC.1 10 FDP_ACF.1-CSPP 17 FDP_RIP.1 18 FDP_SDI.1 21 FIA_AFL.1 22 FIA_ATD.1 23 FIA_SOS.1 24 FIA_SOS.2 25 FIA_UAU.1 26 FIA_UAU.5 27 FIA_UAU.6 28 FIA_UAU.7 29 FIA_UID.1 30 FIA_USB.1 35 FMT_SAE.1 39 FPT_ITC.1-CSPP 40 FPT_ITI.1-CSPP 41 FPT_ITT.1-CSPP 42 FPT_RCV.2 43 FPT_RPL.1 44 FPT_RVM.1 45 FPT_SEP.1 48 FPT_TST.1 50 FTA_LSA.1 52 FTA_SSL.1 54 FTA_SSL.3 55 FTA_TAB.1-CSPP 56 FTA_TAH.1 57 FTA_TSE.1 58 FTP_ITC.1-CSPP 59 FTP_TRP.1-CSPP 60 FPT_SYN-CSPP.1

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.	5 FAU_SAR.3 6 FAU_SEL.1 7 FAU_STG.1 9 FDP_ACC.1 10 FDP_ACF.1 14 FDP_IFF.1 21 FIA_AFL.1 23 FIA_SOS.1 24 FIA_SOS.2 55 FTA_TAB.1 56 FAT_TAH.1
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.	1 FAU_GEN.1 3 FAU_SAR.1 5 FAU_SAR.3 7 FAU_STG.1 18 FDP_SDI.1 21 FIA_AFL.1 43 FPT_RPL.1 51 FPT_MCS.1-CSPP 56 FTA_TAH.1

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.	1 FAU_GEN.1 5 FAU_SAR.3 6 FAU_SEL.1 7 FAU_STG.1 8 FAU_STG.3 9 FAU_ACC.1 10 FDP_ACF.1 11 FDP_DAU.1 12 FDP_ETC.1 14 FDP_IFF.1 17 FDP_RIP.1 21 FIA_AFL.1 23 FIA_SOS.1 24 FIA_SOS.2 30 FIA_USB.1 31 FMT_MOF.1 32 FMT_MSA.1 33 FMT_MSA.3 34 FMT_MTD.1 35 FMT_SAE.1 36 FMT_SMR.1 45 FPT_SEP.1 48 FPT_TST.1 50 FTA_LSA.1 51 FTA_MCS.1 52 FTA_SSL.1 53 FTA_SSL.2 54 FTA_SSL.3 55 FTA_TAB.1 56 FTA_TAH.1
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.	14 FDP_IFF.1
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.	1 FAU_GEN.1 5 FAU_SAR.3 6 FAU_SEL.1 8 FAU_STG.3 31 FMT_MOF.1 32 FMT_MSA.1 33 FMT_MSA.3 34 FMT_MTD.1 35 FMT_SAE.1 386 FMT_SMR.1

O.NETWORK: The system must be able to meet its security objectives in a distributed environment. This will be accomplished with high effectiveness.	15 FDP_ITC.1 16 FDP_ITT.1 19 FDP_UCT.1 20 FDP_UIT.1 26 FDP_UAU.5 39 FPT_ITC.1 40 FPT_ITI.1 41 FPT_ITT.1 43 FPT_RPL.1 46 FPT_TDC.1 47 FPT_TRC.1 58 FTP_ITC.1 59 FTP_TRP.1 60 FPT_CSPP.1
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.	1 FAU_GEN.1 5 FAU_SAR.3 6 FAU_SEL.1 53 FTA_SSL.2
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, but the majority of the focus will be on detection and response, with high effectiveness for specified failures. For general failure, this will be accomplished with low effectiveness.	8 FAU_STG.3 18 FDP_SDI.1 38 FPT_FLS.1 42 FPT_RCV.2 48 FPT_TST.1

4.4 Strength of Function (SOF)

4.4.1 Minimum SOF Claim

The basic design goal for CSPP was to produce a requirement set that is suitable for near-term implementation with commercial off the shelf products. The selection of ***basic*** as the minimum level is clearly a direct result of this goal.

4.4.2 Specific SOF Claims

The specific SOF claims are all within the category of currently, and widely available. All represent at least a ***basic*** level of strength.

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.

4.3 CORRECT TOE FUNCTIONALITY

4.3.1 Dependencies for TOE functionality

Table 4.3.1-1 shows correctness of the TOE functional set with respect to meeting all dependencies.

Table 4.3.1-1 Correct TOE Functionality – Dependency Mapping

#	CSPP Functional Component	Name	Dependency	CSPP Function #
1	FAU_GEN.1-CSPP	Audit data Generation	FPT_CSPP.1	60
2	FAU_GEN.2	User Identity Generation	FAU_GEN.1 FIA_UID.1	1 29
3	FAU_SAR.1	Audit Review	FAU_GEN.1	1
4	FAU_SAR.2	Restricted Audit Review	FAU_SAR.1	3
5	FAU_SAR.3	Selectable Audit Review	FAU_SAR.1	3
6	FAU_SEL.1-CSPP	Selective Audit	FAU_GEN.1 FMT_MTD.1	1 34
7	FAU_STG.1	Protected audit trail storage	FAU_GEN.1	1
8	FAU_STG.3	Action in case of Possible Audit Data Loss	FAU_STG.1	7
9	FDP_ACC.1	Subset Access Control	FDP_ACF.1	10
10	FDP_ACF.1-CSPP	Security Attribute Based Access Control	FDP_ACC.1 FMT_MSA.3	9 33
11	FDP_DAU.1	Basic data authentication	—	—
12	FDP_ETC.1-CSPP	Export of user data without security attributes	FDP_ACC.1 FDP_IFC.1	9 14
13	FDP_IFC.1	Subset information flow control	FDP_IFF.1	15
14	FDP_IFF.1	Simple security attributes	FDP_IFC.1 FMT_MSA.3	14 33
15	FDP_ITC.1	Import of user data without security attributes	FDP_ACC.1 FDP_IFC.1 FMT_MSA.3	9 14 33
16	FDP_ITT.1	Basic internal transfer protection	FDP_ACC.1 FDP_IFC.1	9 14
17	FDP_RIP.1	Subset Residual Information protection	—	—
18	FDP_SDI.1	Stored data integrity monitoring	—	—
19	FDP_UCT.1	Basic data exchange confidentiality	FTP_ITC.1 FTP_TRP.1 FDP_ACC.1 FDP_IFC.1	58 59 9 13

#	CSPP Functional Component	Name	Dependency	CSPP Function #
20	FDP_UIT.1	Data exchange integrity	FTP_ITC.1 FTP_TRP.1 FDP_ACC.1 FDP_IFC.1	58 59 9 13
21	FIA_AFL.1	Authentication Failure Handling	FIA_UAU.1	25
22	FIA_ATD.1	User Attribute Definition	—	—
23	FIA_SOS.1	Verification of Secrets	—	—
24	FIA_SOS.2	TSF Generation of Secrets	—	—
25	FIA_UAU.1	Timing of authentication	FIA_UID.1	29
26	FIA_UAU.5	Multiple authentication mechanisms	—	—
27	FIA_UAU.6	Re-authenticating	—	—
28	FIA_UAU.7	Protected authentication feedback	FIA_UAU.1	25
29	FIA_UID.1	Timing of identification	—	—
30	FIA_USB.1	User-Subject Binding	FIA_ATD.1	23
31	FMT_MOF.1	Management of security functions behavior	FMT_SMR.1	36
32	FMT_MSA.1	Management of security attributes	FDP_ACC.1 FDP_IFC.1 FMT_SMR.1	9 13 36
33	FMT_MSA.3	Static attribute initialization	FMT_MSA.1 FMT_SMR.1	32 36
34	FMT_MTD.1	Management of TSF data	FMT_SMR.1	36
35	FMT_SAE.1	Time-Limited Authorization	FMT_SMR.1 FMT_CSPP.1	36 60
36	FMT_SMR.1	Security roles	FIA_UID.1	29
37	FPT_AMT.1	Abstract Machine Testing	—	—
38	FPT_FLS.1	Failure with preservation of secure state	ADV_SPM.1	PP Sec 6.0
39	FPT_ITC.1-CSPP	Inter-TSF Confidentiality During Transmission	—	—
40	FPT_ITI.1-CSPP	Inter-TSF detection of modification	—	—
41	FPT_ITT.1-CSPP	Basic internal TSF data transfer protection	—	—
42	FPT_RCV.2	Automated Recovery	ADV_SPM.1 AGD_ADM.1 FPT_TST.1	PP Sec 6.0 PP Sec 6.0 48
43	FPT_RPL.1	Replay detection	—	—
44	FPT_RVM.1	Non-Bypassability of the TSP	—	—
45	FPT_SEP.1	TSF Domain Separation	—	—
46	FPT_TDC.1	Inter-TSF basic TSF data consistency	—	—

#	CSPP Functional Component	Name	Dependency	CSPP Function #
47	FPT_TRC.1	Internal TSF consistency	FPT_ITT.1	41
48	FPT_TST.1	TSF Testing	FPT_AMT.1	37
49	FRU_RSA.1-CSPP	Maximum quotas	—	—
50	FTA_LSA.1	Limitation on scope of selectable attributes	—	—
51	FTA_MCS.1-CSPP	Basic limitation on multiple concurrent session	FIA_UID.1	29
52	FTA_SSL.1	TSF-initiated session locking	FIA_UAU.1	25
53	FTA_SSL.2	User-initiated locking	FIA_UAU.1	25
54	FTA_SSL.3	TSF-initiated termination	—	—
55	FTA_TAB.1-CSPP	Default TOE access banners	—	—
56	FTA_TAH.1	TOE access history	—	—
57	FTA_TSE.1	TOE session establishment	—	—
58	FTP_ITC.1-CSPP	Inter-TSF trusted channel	—	—
59	FTP_TRP.1-CSPP	Trusted path	—	—
60	FPT_SYN-CSPP.1	TSF synchronization	—	—

4.3.2 TOE Functional Operations

Table 4.3.2-1 provides the rationale for the operations performed on the TOE functional components. Not included in this table are deferred operations (to include completed operations related to deferred information) and extensions (to include deferred operations related to the extensions). These are covered in tables 4.3.2-2 and 4.3.2-3 respectfully.

Table 4.3.2-1 Correct TOE Functionality – Rationale for Operations Performed

Functional Operations Performed in PP	**Rationale**
FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: b) All auditable events relevant for the [**selection:** basic] level of audit; and	Selection - "basic" is most appropriate considering the basic assurance goals for CSPP.
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, and [**selection:** success, 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:** the identity of the process acting on behalf of a user or of the system, and the subject's user group for this access].	Selection - indication of success or failure is an important item of audit information. Assignment - these two additions are considered important.
FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the individual identity of the user or system process that caused the event.	Refinement - in addition to users, the system must be able to identify the process that generated the auditable event.
FAU_SAR.1.1 The TSF shall provide [**assignment:** explicitly authorized user roles, user groups, or individually identified users] with the capability to read [**assignment:** all information in the audit records] from the audit records.	Selection - all three CC choices are appropriate for CSPP. Assignment: for the level of granularities of this PP guidance, 'all' is considered appropriate.
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].	Selection - all three CC choices apply. Refinement - editorial. Assignment - these are the basic items upon which a search would be conducted.
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].	Selection - all CC choices are appropriate. Refinement - editorial. Assignment - these are the other two elements that should be selectable.

Functional Operations Performed in PP	Rationale
FAU_STG.1.2 The TSF shall be able to [**selection:** prevent and detect] modifications to the audit records.	Selection - both CC choices are appropriate.
FAU_STG.3.1 The TSF shall take [**assignment:** the action to notify an identified user or console of the possible audit data loss] if the audit trail exceeds [**assignment:** an authorized user selectable, pre-defined limit].	Assignment - this is the generic action. Assignment - rather that specify a limit, it should be a system parameter.
FDP_ACC.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP] on …	Assignment - this is the generic policy to enforce.
FDP_ACF.1.1 The TSF shall enforce the [**assignment:** CSPP 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].	Assignment - this is the generic policy. Assignment - this is a reasonable, near-term COTS requirement.
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].	Assignment - this is a basic statement of access control.
FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**assignment:** none].	Assignment - no other rules are needed.
FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**assignment:** none].	Assignment - no other rules are needed.
FDP_ETC.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP and …] when exporting user data, controlled under the SFP, outside of the TSC.	Assignment - this is the generic policy.
FDP_ITC.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP and …] when importing user data, controlled under the SFP, from outside the TSC.	Assignment - this is the generic policy.
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].	Assignment - this is a commonly available, and useful capability.

Functional Operations Performed in PP	Rationale
FDP_ITT.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP and … to prevent the …[**selection:** modification, loss of use] of user data when it is transmitted between physically-separated parts of the TOE.	Assignment - this is the generic policy. Selection - these are the two CC choices that will definitely apply. The third 'disclosure' is left to the PP to specify as it is policy specific.
FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the … the following objects [**assignment:** shared memory and file storage space and the items defined in the following ST assignment ….	Assignment - these are the two most common resources. Others can be specified as a deferred operation.
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] on all objects, based on the following …	Assignment - for the lower assurance CSPP provides, this is the extend of what can be reasonably expected.
FDP_UCT.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP and … to be able to [**selection:** transmit and receive] objects in a manner protected from unauthorized disclosure.	Assignment - this is the generic policy. Selection - both CC choices are appropriate. Refinement - editorial.
FDP_UIT.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP and …] to be able to [**selection:** transmit and receive] user data in a manner protected from [**selection:** modification, deletion, insertion, and replay] errors.	Assignment - this is the generic policy. Selection - both CC choices are appropriate. Refinement - editorial. Selection - all CC choices are appropriate. Refinement - must protect from all.
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.	Selection - all CC choices are appropriate. Refinement - must detect any.
FIA_AFL.1.1 The TSF shall detect when [**assignment:** an authorized user configurable number of] unsuccessful authentication attempts 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 …].	Assignment - this should a system parameter, not a fixed number. Refinement - there should be a limit after which the user can still logon (to help mitigate denial of service attacks). Assignment - these are the two obvious requirements.
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 …].	Assignment - these are the two obvious items.
FFIA_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	Assignment - as passwords are common, requirements for them are given.

Functional Operations Performed in PP	Rationale
112; for other secrets specific to the ST design…].	
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 …].	Assignment - as passwords are common, requirements for them are given.
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] to support user authentication.	Assignment - this is an expression of the desired requirement.
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 …].	Assignment - at the level of abstraction of this guidance document, the generic requirement seems appropriate. The PP author would include any policy items that apply here.
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,] …].	Assignment - these are the two obvious items.
FIA_UAU.7.1 The TSF shall only provide [**assignment:** no indication of success or failure and no clear-text display of any secret authenticator] to the user while the authentication is in progress.	Assignment - this is the basic requirement.
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 CSPP-OS and for which the common criteria indicates security management suggestions, and also all items listed in the following ST assignment …] to …	Selection - all CC choices are appropriate. Assignment - the CC recommended items are appropriate.
FMT_MSA.1.1 The TSF shall enforce the [**assignment:** CSPP 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 …] 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 …]. See iteration for restriction on read access	Assignment - this is the generic policy. Selection - all CC choices except 'read', which is handled in the iteration, are appropriate. Refinement - editorial. Assignment - 'null' is appropriate. Assignment - this is the basic need. Assignment - this describes the basic need. Refinement - provides information related to

Functional Operations Performed in PP	Rationale
to authenticator values.	the iteration, editorial.
Iteration: FMT_MSA.1.1 The TSF shall enforce the [**assignment:** CSPP 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].	Assignment - this is the generic policy. Selection - this iteration covers 'read'. Assignment - 'null' is appropriate. Assignment - the issue is authenticators. Assignment - users do not need them and only few processes need them.
FMT_MSA.3.1 The TSF shall enforce the [**assignment:** CSPP access control SFP and …] to provide [**assignment:** restrictive] default values for object security attributes that are used to enforce the SFP.	Assignment - this is the generic policy. Assignment - restrictive is considered the desired default.
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.	Assignment - this is the basic requirement.
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].	Selection - all CC choices are appropriate. Assignment - this is the basic requirement. Assignment - access must be through an authorized process.
FMT_SAE.1.1 The TSF shall restrict the ability to specify an expiration time for [**assignment:** user account and authenticators and …] to [**assignment:** an explicitly specified set of users, enforcing least privilege on the basis of the following ST selection …].	Assignment - these are the obvious ones. Assignment - who has access needs to be explicit.
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 …] after the expiration time for the indicated security attribute has passed.	Assignment - this is the basic need.
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 …].	Assignment - this is the reasonable expectation for near-term COTS.
FPT_AMT.1.1 The TSF shall run a suite of tests [**selection:** during initial start-up and at the request of explicitly authorized security administrator(s) or security	Selection - these two are the reasonable expectations for near-term COTS.

Functional Operations Performed in PP	Rationale
administrator role(s)], … to demonstrate the correct …	Refinement - clarify 'authorized user'.
Refinement - added element, clarifying intent: FPT_TDC.1.3-CSPP The TSF shall support maintaining consistent 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.	Refinement - this new element clarifies the intent of the CC component. The component includes requirement for consistent syntax and interpretation. The CC component does not require mechanisms to enforce consistency.
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)] and … and [***assignment:*** *"null"*] to demonstrate the correct operation of the TSF.	Selection - these two are the reasonable expectations for near-term COTS. Refinement - clarify 'authorized user'. Assignment - 'null' is appropriate.
FRU_RSA.1.1-CSPP The TSF shall enforce quotas limiting the maximum quota of the following resources: … that [**selection:** an individual user, a defined group of users, subjects] can use …	Selection - all CC choices are appropriate.
FTA_MCS.1.2 If the TOE is to restrict the maximum number of concurrent sessions, the TSF shall enforce [**assignment:** an authorized user selected maximum number of] sessions per user.	Assignment - it is considered more appropriate to make this a parameter.
FTA_SSL.1.1 The TSF shall lock an interactive session after [**assignment*:*** an authorized user specified time interval of user inactivity] by: …	Assignment - it is considered more appropriate to make this a parameter.
FTA_SSL1.2 The TSF shall require the following events to occur prior to unlocking the session: [**assignment:** user authentication].	Assignment - this is the basic requirement.
FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: [**assignment:** user authentication].	Assignment - this is the basic requirement.
FTA_SSL.3.1 The TSF shall terminate an interactive session after [**assignment*:*** an authorized user specified time interval of user inactivity].	Assignment - it is considered more appropriate to make this a parameter.
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.	Selection - all CC choices are appropriate. Refinement - editorial.
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	Selection - all CC choices are appropriate. Refinement - editorial.

Functional Operations Performed in PP	Rationale
establishment and the … 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 …]. FTP_TRP.1.3 The TSF shall require the use of the trusted path for [**selection:** initial user authentication, user re-authentication,] […].	 Assignment - it is necessary to both define who can set these and to give a generic list. Additional items may be added through the deferred operation. Selection - this is the basic requirement.

Table 4.3.2-2 Correct Functionality – Rationale for Deferring Operations to PP or ST

Functional Operations Deferred to PP or ST	Rationale for Deferring to PP or ST
FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: c) [**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")] d) *[**ST assignment:** as required by the PP, other ST specific auditable events]*	Only at the ST will specific details of the design be known. Therefore, specification of audits related to these details must be deferred.
FDP_ACC.1.1 The TSF shall enforce the … 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]*].	It is not apparent at the abstraction level for this guidance document what the proper list of items should be. A PP author would provide what information is known, in addition to possibly deferring to the ST.
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]*].	It is not apparent at the abstraction level for this guidance document what the proper list of items should be. A PP author would provide what information is known, in addition to possibly deferring to the ST.
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 assignment] 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.	It is not apparent at the abstraction level for this guidance document what the proper list of items should be. A PP author would provide what information is known, in addition to possibly deferring to the ST.
FDP_ETC.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP and *[**PP assignment:** information flow control SFP]*] when exporting user data, controlled under the SFP, outside of the TSC.	It is a PP decision as to whether an information flow control policy applies. (The CSPP access control policy is considered generic enough to call out explicitly.)
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 assignment], and [**ST assignment:** as required by PP, list of ST specific subjects, objects and operations among subjects and objects covered by the*	It is a PP decision as to whether an information flow control policy applies. (The CSPP access control policy is considered generic enough to call out explicitly.) It is not apparent at the abstraction level for this guidance document what the proper list

Functional Operations Deferred to PP or ST	Rationale for Deferring to PP or ST
SFP]].	of items should be. A PP author would provide what information is known, in addition to possibly deferring to the ST.
FDP_IFF.1.1 The TSF shall enforce the [**assignment:** *[**PP assignment:** information flow control SFP]*] to enforce at least 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 assignment] and [**ST assignment:** as required by PP, the ST specific minimum number and type of security attributes]*].	Rationale: Same as for FDP_IFC.1.1
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 assignment] and [**ST assignment:** as required by PP, for each operation, any ST specific security attribute-based relationship that must hold between subject and object security attribute]*].	It is not apparent at the abstraction level for this guidance document what the proper list of items should be. A PP author would provide what information is known, in addition to possibly deferring to the ST.
FDP_IFF.1.3 The TSF shall enforce the [**assignment:** *[**PP assignment:** additional information flow control SFP rules]*].	It is a PP decision as to whether an information flow control policy applies.
FDP_IFF.1.4 The TSF shall enforce the following [**assignment:** *[**PP assignment:** list of additional SFP capabilities]*].	It is not apparent at the abstraction level for this guidance document what the proper list of items should be. The PP author should complete this list.
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]*].	It is not apparent at the abstraction level for this guidance document what the proper list of items should be. The PP author should complete this list.
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]*].	It is not apparent at the abstraction level for this guidance document what the proper list of items should be. The PP author should complete this list.
FDP_ITC.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP and *[**PP assignment:** information flow control SFP]*] when importing user data, controlled under the SFP, from outside the TSC.	It is a PP decision as to whether an information flow control policy applies. (The CSPP access control policy is considered generic enough to call out

Functional Operations Deferred to PP or ST	Rationale for Deferring to PP or ST
	explicitly.)
FDP_ITT.1.1 The TSF shall enforce the [**assignment:** … and *[**PP assignment:** information flow control SFP]*] to prevent the *[**PP selection:** disclosure,]* […] of user data when it is transmitted between physically-separated parts of the TOE.	It is a PP decision as to whether an information flow control policy applies. Protection from 'disclosure' is a policy decision that is not generic enough to specify in this guidance.
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 CSPP design goals): *[**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): *[**ST assignment:** as required by PP, ST specific list of objects]*].	It is generally not important, at the level of abstraction of a PP, which selection is made. It is important that the ST be explicit and ensure that the selection is consistent with the design. Shared memory and file space are the two most common resource and may be sufficient. Knowledge of the design is necessary to determine whether more need to be identified - hence the deferral to the ST with justification required.
FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for […] on all objects, based on the following [**assignment:** *[**ST selection:** all user data, data for which integrity protection has been explicitly requested]*].	If the PP author must meet policy specific to this area, then the selection would not be deferred. But in general, the organizations policy is not likely to specify this in great enough detail and the decision is better left to the ST where the details of the design can be taken into account for a cost-effective implementation.
FDP_UCT.1.1 The TSF shall enforce the [**assignment:** … and *[**PP assignment:** information flow control SFP]*] to be able to ….	It is a PP decision as to whether an information flow control policy applies.
FDP_UIT.1.1 The TSF shall enforce the [**assignment:** … and *[**PP assignment:** information flow control SFP]*] to be able to …	It is a PP decision as to whether an information flow control policy applies.
FIA_AFL.1.1 The TSF shall detect when … 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):*[**ST assignment:** as required by PP, list of ST specific authentication events]*].	Login and re-authentication are the two obvious choices. The details of the design may indicate additional choices - hence the deferral to the ST with justification required.

Functional Operations Deferred to PP or ST	Rationale for Deferring to PP or ST
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]*].	As the assignment indicates, it is not particularly important at the level of abstraction of this guidance document, and probably most PPs, which selection is made. It is important that the choice be explicit and consistent with the design. If the PP author has specific policy to meet in this area, then the selection will be completed in the PP and not deferred.
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"): *[**ST assignment:** as required by PP, list of ST specific security attributes]*].	The two items listed are fairly obvious. Additional items can be derived from other requirements, yet there remains a need to consider specifics of the design - hence the deferral to the ST with justification required.
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 CSPP design goals): *[**ST assignment:** as required by PP, any ST specific, defined quality metrics]*].	Since passwords are so common, guidance is provided. However, other secrets used are highly dependent on the design - hence the deferral to the ST with justification required.
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 assignment] [**ST assignment:** as allowed by PP, a ST specific, defined quality metric]*].	Since passwords are so common, guidance is provided. However, other secrets used are highly dependent on the design - hence the deferral to the ST with justification required.
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 assignment] [**ST assignment:** as required by PP, a ST specific, list of TSF functions]*].	The list of secrets used is highly dependent on the design - hence the deferral to the ST with justification required.
FIA_UAU.1.1 The TSF shall allow [**assignment:** *[**PP**	It is highly policy specific what actions are

Functional Operations Deferred to PP or ST	Rationale for Deferring to PP or ST
assignment: *list of TSF mediated actions and sufficient information for ST author to make a compliant, ST specific assignment] [**ST 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.	allowed prior to authentication. Hence this is deferred to the PP, with a potential for additional information provided in the ST.
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): *[**ST assignment:** as required by PP, rules describing how the multiple authentication mechanisms provide authentication]*].	This assignment provides for flexibility in the use of multiple mechanisms. By deferring to the ST, a most cost-effective solution is enabled. By requiring ST justification of the choices made, compliance is verifiable.
FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions … [**assignment:** 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): *[**ST assignment:** as required by PP, list of other, ST specific conditions under which re-authentication is required]*].	This assignment provides for the possibility of additional, design-specific conditions, over those explicitly stated - hence the deferral to the ST with justification required.
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.	This is policy specific and therefore deferred to the PP, with the possibility of addition information in the ST.
FMT_MOF.1.1 The TSF shall restrict the ability to … the functions [**assignment:** included as requirements for CSPP-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 specifics of the design may indicate additional management needs - hence the deferral to the ST with justification required. By providing this option to the ST, a degree of flexibility is provided that can result in a more cost-effective implementation, without risk of non-compliance with basic CSPP security goals.

Functional Operations Deferred to PP or ST	Rationale for Deferring to PP or ST
FMT_MSA.1.1 The TSF shall enforce the … 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 rationale for FMT_MOF.1.1.
FMT_MSA.3.1 The TSF shall enforce the [**assignment:** … and *[**PP assignment:** information flow control SFP]*] to provide … default values for object security attributes that are used to enforce the SFP.	It is a PP decision as to whether an information flow control policy applies.
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"), *[**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): *[**ST assignment:** as allowed by PP, the ST specific authorized identified roles]*].	In addition to the two obvious items mentioned, the design may require additional item - hence the deferral to the ST with justification required. By providing this option to the ST, a degree of flexibility is provided that can result in a more cost-effective implementation, without risk of non-compliance with basic CSPP security goals.
FMT_SAE.1.2 For each of these security attributes, TSF shall be able to … 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.	This deferral allows for the potential of design specific items in addition to those given.
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 CSPP goals and useful in implementing these goals (the ST author must provide a basic justification that the roles specified do not conflict with CSPP design goals): *[**ST assignment:** as allowed by PP,*	By providing this option to the ST, a degree of flexibility is provided that can result in a more cost-effective implementation, without risk of non-compliance with basic CSPP security goals.

Functional Operations Deferred to PP or ST	Rationale for Deferring to PP or ST
the ST specific authorized identified roles]].	
FPT_AMT.1.1 The TSF shall run a suite of tests …, *[**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 provided by the abstract machine which underlies the TSF.	As it is questionable whether this will be included in near-term COTS, it is a PP decision as to whether this selection is to be included along with the other given. Additionally, the assignment expects the PP authors to have additional information and recognizes that there may be design specific items - hence the deferral to the ST.
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: *[**ST assignment:** as required by PP, list of ST specific types of TSF failures]*].	It is felt that the primary purpose of the requirement is to know from which failures the TOE can recover, rather than to specify the set of failures. Hence the deferral to the ST.
FPT_ITI.1.1-CSPP The TSF shall provide the capability to detect modification of … 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]*].	The definition of such metrics is not feasible at the level of abstraction of this guidance document. It is expected that the PP author will have information related to policy and common practices to use in completing this operation. Also, there is the potential for additional design specific information - hence the possible deferral to the ST.
FPT_ITI.1.2-CSPP The TSF shall provide the capability to verify the integrity of … 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.	CSPP may eventually provide a suggested list of actions. But at this time, the PP author must complete this operation. Additionally, there is the potential for design specific items and hence the possible deferral to the ST.
FPT_ITT.1.1-CSPP The TSF shall protect TSF data from *[**PP selection:** disclosure, modification]* and … when it is transmitted between separate parts of the TOE.	In addition to the selections made, the PP author will need to apply policy to determine whether disclosure and modification need to be included.
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.	It is felt that the primary purpose of the requirement is to know from which failures the TOE can automatically recover, rather than to specify the set of failures. Hence the deferral to the ST.
FPT_RPL.1.1 The TSF shall detect replay for the following entities [**assignment:** *[**PP assignment:** list of*	It is expected that the PP author will have information related to policy and common

Functional Operations Deferred to PP or ST	Rationale for Deferring to PP or ST
*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]*].	practices to use in completing this operation. Also, there is the potential for additional design specific information - hence the possible deferral to the ST.
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.	It is expected that the PP author will have information related to policy and common practices to use in completing this operation. Also, there is the potential for additional design specific information - hence the possible deferral to the ST.
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.	The PP author may have additional information on specific data types, or may choose to have the designer develop this list and provide a justification that the list is complete.
FPT_TDC.1.2 The TSF shall use [**assignment:** *[**PP assignment:** list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.	The PP author will be able to apply specific policy in light of the choices made for FPT_TDC.1.1 above.
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]*].	The specific nature of the TOE is likely to influence this list, hence deferral to the PP. It is also noted, the specifics of the design could impact the list, necessitating the potential for added information in the ST.
FPT_TST.1.1 The TSF shall run a suite of self tests … *[**PP selection:** periodically during normal operation]* … to demonstrate the correct operation of the TSF.	As it is questionable whether this will be included in near-term COTS, it is a PP decision as to whether this selection is to be included along with the other given.
FRU_RSA.1.1-CSPP The TSF shall enforce 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 … can use *[**PP selection:** simultaneously, over a specified period of time]*.	The PP author may have information available that allows specific items to be included in this list. In general, however, this is likely to be highly dependent on the design and hence the potential for deferral to the ST for additional details. The PP author will apply policy details to make the selection.
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*	The PP author may have information available that allows specific items to be

Functional Operations Deferred to PP or ST	Rationale for Deferring to PP or ST
*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]*].	included in this list. In also possible that this will be influenced by the design and hence the potential for deferral to the ST for additional details.
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]*].	The assignment makes the requirement that this be settable, rather than fixed. This is considered essential. Also, in addition to the four items given, the PP author may have policy requirements that identify additional items. Finally, there may be design specific items and hence the possible deferral to the ST.
FTP_ITC.1.2 The TSF shall permit *[**PP selection:** the TSF, the remote trusted IT product]* to initiate communication via the trusted channel.	The PP author needs to decide which choices are necessary and which choices are feasible with respect to the type of TOE for that PP.
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]*].	The PP author may have information available that allows specific items to be included in this list. In also possible that this will be influenced by the design and hence the potential for deferral to the ST for additional details.
FTP_TRP.1.1-CSPP 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 …communicated data from disclosure.	The PP author needs to decide which choices are necessary and which choices are feasible with respect to the type of TOE for that PP.
FTP_TRP.1.2 The TSF shall permit *[**PP selection:** the TSF, local users, remote users]* to initiate communication via the trusted path.	The PP author needs to decide which choices are necessary and which choices are feasible with respect to the type of TOE for that PP.
FTP_TRP.1.3 The TSF shall require the use of the trusted path for … [**assignment:** 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]*].	The PP author may have information available that identifies other specific items to be included. In also possible that this will be influenced by the design and hence the potential for deferral to the ST for additional details.

Table 4.3.2-3 gives the rationale for each functional extension included in CSPP.

Table 4.3.2-3 Correct Functionality – Rationale for Functional Extensions

Functional Extension	**Rationale for the Extension**
FAU_GEN.1-CSPP.3 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.	Some required auditing can only be performed by the application. A common audit trail is extremely important. Therefore the FAU-GEN1.3 extension is an important part of CSPP auditing, especially in the context of a distributed system.
FAU_SEL.1-CSPP.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.	This element provides useful additional information and provide a good "handle" for the next extension.
FAU_SEL.1-CSPP.3 The TSF shall provide the capability of FAU_SEL.1-CSPP.2 at any time during the operation of the TOE.	It is important that the system allow for audit selection during operation. Responding to real-time events without having to bring the system down necessitates this capability.
FDP_ACF.1-CSPP.5 The TSF shall provide the capability to assign a user to be a member of more than one user group simultaneously.	The practical application of role-based controls, or the effective use of group membership necessitates this requirement.
FDP_ACF.1-CSPP.6 The TSF shall enforce the rules for authorizing and denying access based upon the CSPP precedence rules.	It is very important that the access control decision be clearly defined and well understood. An explicit set of precedence rules is essential to making this happen.
FDP_ETC.1-CSPP.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 from outside the TSC.	It is a common capability to provide for such information channels. Existing CC elements do not provide a means to call out this requirement.
FPT_ITC.1.1-CSPP The TSF shall protect [**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): *[**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.	It is considered important to allow for a subset of information to be protected, rather than the CC requirement for 'all'. Clearly 'authenticators' should be protected. At the PP level of abstraction it is not clear which other items require such protection, hence the deferral to the ST.

Functional Extension	**Rationale for the Extension**
FPT_ITI.1.1-CSPP The TSF shall provide the capability to detect modification of [**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]*] data during transmission between TSF and a remote trusted IT product …	It is considered important to allow for a subset of information to be protected, rather than the CC requirement for 'all'. At the PP level of abstraction it is not clear which items require such protection, hence the deferral to the ST.
FPT_ITI.1.2-CSPP The TSF shall provide the capability to verify the integrity of [**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 …	It is considered important to allow for a subset of information to be protected, rather than the CC requirement for 'all'. At the PP level of abstraction it is not clear which items require such protection, hence the deferral to the ST.
FPT_ITT.1.1-CSPP The TSF shall protect TSF data from … and [**extension*****: [PP selection:*** *deletion, replay]*] when it is transmitted between separate parts of the TOE.	In addition to the CC choices, it is considered important to add 'deletion and replay' to the list. It is a policy decision to be determined with the PP whether these apply. Since this changes the requirement, it is marked as an extension rather than a refinement.
FPT_SYN-CSPP.1.1 The TSF shall provide the capability to synchronize distributed TSF elements and to associate audit event records produced by multiple TSF entities.	The existing CC component requires a synchronized time-stamp. While this is the mostly likely underlying mechanism to accomplish synchronization, the true requirement is to synchronize. Hence this new FPT component. Not that the existing CC component can be met by providing the time-stamp mechanism without the need of actually using it to achieve synchronization. The ability to configure the warning banner is an essential requirement as organizational needs change over time.
FTA_MCS.1.1-CSPP The TSF shall [**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 …	It is considered important to allow the organization to decide whether to restrict the number of session. The CC does not currently allow this and hence this extension. Since this changes the requirement, it is marked as an extension rather than a refinement.
FTA_TAB.1-CSPP.2 The TSF shall provide the capability for an authorized user to specify and subsequently modify the contents of this warning message.	It is essential the message be modifiable. Laws, regulations, policies, and needs change over time.

Functional Extension	**Rationale for the Extension**
FTP_ITC.1.1-CSPP 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 [**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 [**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.	It is considered important to allow for a subset of information to be protected, rather than the CC requirement for 'all'. At the PP level of abstraction it is not clear which items require such protection, hence the deferral to the ST.
FTP_TRP.1.1-CSPP The TSF shall provide a communication path between itself and … users that is logically distinct from other communications paths and provides assured identification of its end points and protection of the [**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 [**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.	It is considered important to allow for a subset of information to be protected, rather than the CC requirement for 'all'. At the PP level of abstraction it is not clear which other items require such protection, hence the deferral to the ST.

5.0 ASSURANCE REQUIREMENTS RATIONALE

5.1 NECESSARY ASSURANCES

5.1.1 Basic Assurance Goals

CSPP provides a definition for near-term achievable, low evaluation cost, COTS security. In keeping with this purpose, the assurance components of this protection profile have been selected to (1) require only current best-practice development actions and (2) include minimal third-party analysis. The rationale for each is given below.

It is clearly evident that, in order to meet "near-term achievable", requirements placed upon the developer must be constrained. The current COTS development standards do not include security engineering to any significant degree. Adding such techniques and processes would require changes to development practices and personnel capabilities. Since such changes are not considered likely, CSPP has been developed with that in mind.

The rationale for limiting third-party analysis is:

Technical basis. In keeping with current best commercial practice, CSPP requirements do not include significant security engineering. Therefore, there is no reasonable expectation of high security quality with respect to effectiveness in the face of competent threat agents. Moreover, the most likely internal structures for CSPP components make comprehensive evaluation extremely difficult, if not, for all practical purposes, impossible. Hence, the probability of exploitable vulnerabilities in CSPP compliant components is not significantly different than that of non-compliant COTS. Since there is no reasonable expectation for high security quality in CSPP components (even with an extensive evaluation), there is no technical basis for extensive evaluation of CSPP class components.

Business-case basis. In order to support a good business case, CSPP evaluation must be achievable without negative impact on customer acceptance over non-evaluated competition. Since CSPP vendors cannot reasonably claim high security quality, CSPP evaluation is unlikely to be a discriminator overcoming cost and time-to-market. Hence, the CSPP evaluation provides a market advantage if evaluated products are competitive against non-evaluated products on the basis of cost and time-to-market. Therefore, a CSPP evaluation must be low cost and of short duration.

5.1.2 EAL Selection

This section provides a rationale for the selection of EAL2 as the base EAL for EAL-CSPP. This will be accomplished by first describing why EAL1 is not sufficient and then describing why EAL3 is too much for the basic goals for CSPP. Since the EALs are strictly hierarchical, the rationale for not selecting EAL4 through EAL7 is covered by that given for EAL3.

a. EAL1 not sufficient. Table 5.1.2-1 lists the assurance components contained in EAL2 which are not a part of EAL1, describing why they are required assurances for CSPP. Since EAL1 lacks these components, it is not sufficient as the base EAL.

Table 5.1.2-1 Necessary Assurance - EAL1 Not Sufficient

EAL2 Component not in EAL1	Component Title	Why Required in CSPP
ACM_CAP.2 (EAL-1 has CAP.1)	Configuration items	It is well within best commercial practice for a security product vendor to have CM documentation and to be able to uniquely identify all configuration items. Since it is reasonable to expect this, the assurance it offers should be a part of CSPP.
ADO_DEL.1	Delivery procedures	This component requires that the vendor have procedures for "secure" delivery to the customer. Since (1) software piracy controls will be implemented and (2) the CSPP requirement does not specify a specific set of procedures, this component is within the range of best commercial practice and should be a part of CSPP.
ADO_IGS.1	Installation, generation, and start-up procedures	It is necessary and reasonable to expect an IT security product to include guidance to the user on secure installation, generation, and start-up. Therefore this must be a part of an effective CSPP.
ADV_HDL.1	Descriptive high-level design	If using best commercial practice, the vendor can be expected to have the high-level design for the TSF required by this component. Since it is a reasonable expectation, it should be included in CSPP.
ATE_IND.2 (EAL1 has IND.1)	Independent testing – sample	Having the evaluator execute a sample of the vendor tests, as a check on their validity, is a low-cost, reasonable action well within the bounds of the basic goals for CSPP assurance.
AVA_SOF.1	Strength of TOE security function evaluation	This is a vendor driven requirement, in that the only analysis required is for security functionality for which the security target includes a claim of strength of function. If the claim is not made, no analysis is required. If the claim is made, then requiring an analysis is a reasonable expectation and should be a part of CSPP.
AVA_VLA.1	Developer vulnerability analysis	It is an essential part of the CSPP basic assurance level that at least obvious; and common, public-domain; vulnerabilities are addressed.

b. EAL3 too much. Table 5.1.2-2 lists the assurance components contained in EAL3 which are not a part of EAL2, describing those that are not appropriate for CSPP. Since EAL3 contains these components, it is too much for the base EAL. Because of the hierarchical nature of the EALs, EAL4 through EAL7 are also too much, leaving EAL2 as the best choice.

Table 5.1.2-2 Necessary Assurance - EAL3 Too Much

EAL3 Component Not in EAL2	Component Title	Why not appropriate for CSPP
ACM_CAP.3 (EAL2 has CAP.2)	Authorization controls	N/A – included in EAL-CSPP
ACM_SCP.1	TOE CM coverage	N/A – included in EAL-CSPP as part of the CSPP requirement for ACM_SCP.2
ADV_HLD.2	Security enforcing high-level design	This component is the reason EAL3 is not acceptable as the base level for CSPP. The requirement to "describe the separation of the TSF into TSP enforcing and other subsystems" reflects a degree of and capability for security engineering that is not a part of current (or expected near-term) standard COTS development. Although most of EAL3 is a part of EAL-CSPP, the CC explicitly forbids calling out an EAL subset. Therefore, not wanting this component of EAL3 necessitates going to an augmented version of the next lower EAL (EAL2).
ALC_DVS.1	Identification of security measures	N/A – included in EAL-CSPP
ATE_COV.2 (EAL2 has COV.1)	Analysis of coverage	N/A – included in EAL-CSPP
ATE_DPT.1	Testing: high level design	N/A – included in EAL-CSPP
AVA_MSU.1	Examination of guidance	N/A – included in EAL-CSPP as part of the CSPP requirement for AVA_MSU.3

5.1.3 EAL Augmentation

Table 5.1.3-1 gives the rationale for each CC assurance component in EAL-CSPP that is an augmentation to the base EAL2 level.

Table 5.1.3-1 Necessary Assurance - Augmentation Rationale

Component	Component Title	Rationale for Augmentation
ACM_CAP.3	Authorization controls	Note: EAL2 includes ACM_CAP.2. ACM_CAP.3 adds the requirement for a CM plan and its use. A quality IT vendor developing secure products can be reasonably expected to provide this CM. The use of a CM plan is within the bounds of standard, best commercial practice for IT development.
ACM_SCP.2	Problem tracking CM coverage	Note: EAL2 has no ACM_SCP component. A CSPP vendor can be expected to apply CM to the items called out in ACM_SCP.2. Specifically, since the product is security related, the tracking of security flaws is a very reasonable expectation and within the bounds of standard, best commercial practice.
ADV_SPM.1	Informal TOE security policy model	This assurance component is a required dependency for the following, essential functional requirements: FMT_MSA.3 Static attribute initialization FPT_FLS.1 Failure with preservation of secure state FPT_RCV.2 Automated Recovery While the generation of a security policy does require security expertise, this can be performed by a consultant (if necessary) and does not otherwise impact the vendor's existing development process.
ALC_DVS.1	Identification of security measures	This component requires the definition and implementation of protective security measures during IT development. Since there is no requirement for a specific set of measures, the vendor is largely free to state his procedures as they exist. Therefore, this imposes no undue burden on the vendor and is within the scope of standard, best commercial practice.

Component	Component Title	Rationale for Augmentation
ALC_FLR.2	Flaw reporting procedures	Note: EAL2 has no ALC_FLR component. It is well within standard, best commercial practice for a vendor of security products to have flaw remediation procedures covering acting upon user reports, correcting flaws, notifying users, and reducing the potential for introducing new flaws. Specific procedures are not indicated in the assurance requirement, therefore there is minimal impact on any vendor who is already accomplishing the intent of the requirement.
ATE_COV.2	Analysis of coverage	Note: EAL2 has ALC_COV.1. It is reasonable to require a security vendor implementing best commercial practice to demonstrate that the vendor testing completely covers the security functionality called out in the vendor produced functional specification.
ATE_DPT.1	Testing: high level design	This component requires that the vendor analyze the vendor testing to demonstrate that it verifies the high-level design. For a competent, security vendor implementing best commercial practices, this should be of little impact to existing development activities.
AVA_MSU.2	Validation of analysis	Note: EAL2 has no AVA_MSU component. A security vendor implementing standard, best commercial practices will not be impacted by this component. AVA_MSU.2 requires that the vendor produce user and administrator documentation that is adequate for understanding the operating modes of the TOE and the required external security controls necessary for secure operation. The vendor is required to analyze this documentation for conformance to the requirements. The other AVA_MSU.2 requirements fall onto the evaluator. AVA_MSU.2 is essential in covering T.OBSERVE and is important in covering P.SURVIVE T.CRASH T.INSTALL T.OPERATE

5.2 SUFFICIENT ASSURANCES

Table 5.2-1 maps unused CC assurance components to the rationale for non-selection.

Table 5.2-1 Complete Assurance - Non-Selection Rationale

Component	Component Title	Why Not Included in EAL-CSPP
Family ACM_AUT	CM Automation	While automation of the CM process can be beneficial, it is simply not a key factor in determining the security quality for CSPP compliant TOEs. A vendor can use the fact that his CM includes automated processes as justification for meeting other requirements, but automation is not, itself, a requirement.
ACM_CAP.4 ACM_CAP.5	Generation support and acceptance procedures Advanced support	While the vendor may have CM procedures covering TOE generation (CAP.4) and integration (CAP.5), these are much less likely to be a part of the existing vendor practices than those included with the EAL-CSPP requirement for ACM_CAP.3.
ACM_SCP.3	Development tools CM coverage	Full CM coverage of developmental tools is not a part of standard, best commercial practice and is therefore beyond the scope of the basic goals for CSPP assurance.
ADO_DEL.2 ADO_DEL.3	Detection of modification Prevention of modification	ADO_DEL.2 and DEL.3 are not part of standard, best commercial practice and therefore are beyond the scope of the basic goals for CSPP assurance.
ADO_IGS.2	Generation log	The requirement for a generation log is not a part of standard, best commercial practice and is therefore beyond the scope of the basic goals for CSPP assurance.
ADV_FSP.2 ADV_FSP.3 ADV_FSP.4	Fully defined external interfaces Semiformal functional specification Formal functional specification	While good ideas, fully defined interfaces and semiformal or formal specification are not at part of existing best commercial practice. Therefore these are beyond the scope of the basic goals for CSPP assurance.
ADV_HLD.2 ADV_HLD.3 ADV_HLD.4 ADV_HLD.5	Security enforcing high-level design Semiformal high-level design Semiformal high-level explanation Formal high-level design	The requirements of ADV_HLD.2 include security engineering that is not a part of existing best commercial practices. This is sufficient to make all of these components beyond the scope of the basic goals for CSPP assurance.

Component	Component Title	Why Not Included in EAL-CSPP
Family ADV_IMP	Implementation representation	It is not reasonable, either from the CSPP goal to limit evaluation cost and time or the CSPP goal to keep within the bounds of best commercial practice to include implementation representation requirements.
Family ADV_INT	TSF internals	It is clearly outside the bounds of current best commercial practice to include these requirements on TSF internals. To require these would necessitate major changes to the vendor's development practices. Such changes are beyond the scope of the basic goals for CSPP assurance.
Family ADV_LLD	Low-level design	It is not reasonable, either from the CSPP goal to limit evaluation cost and time or the CSPP goal to keep within the bounds of best commercial practice to include low-level design requirements.
ADV_RCR.2 ADV_RCR.3	Semiformal correspondence demonstration Formal correspondence demonstration	Semiformal or formal requirements are not a part of existing, best commercial practice. Therefore these are beyond the scope of the basic goals for CSPP assurance.
ADV_SMP.2 ADV_SMP.3	Semiformal TOE security policy model Formal TOE security policy model	Semiformal or formal requirements are not a part of existing, best commercial practice. Therefore these are beyond the scope of the basic goals for CSPP assurance.
ALC_DVS.2	Sufficiency of security measures	This requirement may necessitate major changes to existing, vendor development practices, even where standard, best commercial practices are being implemented. Therefore these are beyond the scope of the basic goals for CSPP assurance.
ALC_FLR.3	Systematic flaw remediation	It is beyond best commercial practices to require specific points of contact for flaw reporting and the automatic distribution of flaw reports. Therefore this component is beyond the scope of the basic goals for CSPP assurance.
Family ALC_LCD	Life cycle definition	Current best commercial practices do not include clearly defined life-cycle models. While this may become standard, it is not at present. Therefore this family is beyond the scope of the basic goals for CSPP assurance.

Component	Component Title	Why Not Included in EAL-CSPP
Family ALC_TAT	Tools and techniques	Current best commercial practices do not include these requirements on the definition and control of all tools used in the development. Moreover, this family has ADV_IMP as a required dependency and, as already explained, ADV_IMP is beyond the scope of the basic goals for CSPP assurance.
ATE_COV.3	Rigorous analysis of coverage	It is well outside the bounds of current, best commercial practices to require a rigorous analysis of vendor testing. Therefore this component is beyond the scope of the basic goals for CSPP assurance.
ATE_DPT.2 ATE_DPT.3	Testing – low level design Testing – implementation representation	Since the low-level design and implementation requirements are beyond scope and not included in CSPP, these depth of testing requirements are also beyond the scope of the basic goals for CSPP assurance.
ATE_FUN.2	Ordered functional testing	The requirement for analysis of test ordering dependencies is not part of best commercial practices and hence is beyond the scope of the basic goals for CSPP assurance.
ATE_IND.3	Independent testing – complete	This requirement adds unnecessary time and cost to the evaluation. Therefore it is beyond the scope of the basic goals for CSPP assurance.
Family AVA_CCA	Covert channel analysis	Covert channel analysis is not a part of existing best commercial practice and therefore is beyond the scope of the basic goals for CSPP assurance.
AVA_MSU.3	Analysis and testing for insecure states	While this component might be considered within the range of best commercial practices, it is outside the scope of near-term, mutual recognition agreements and hence has not been selected for CSPP.
AVA_VLA.2 AVA_VLA.3 AVA_VLA.4	Independent vulnerability analysis Moderately resistant Highly resistant	The requirements already a part of CSPP through AVA_VLA.1 include evaluator penetration testing, and additional evaluator actions would be beyond the scope of the basic goals for CSPP assurance. Moreover, the reasonable expectations for CSPP compliant TOEs do <u>not</u> include the potential for resistance to penetration.
AMA_AMP	Assurance maintenance plan	This family is beyond the scope of the basic goals for CSPP assurance.
AMA_CAT	TOE component categorization report	While a case can be made for inclusion of this family as part of CSPP, AMA_CAT is not covered by near-term, mutual recognition agreements and is therefore excluded from CSPP.

Component	Component Title	Why Not Included in EAL-CSPP
AMA_EVD	Evidence of assurance maintenance	This family does not apply to an initial evaluation.
AMA_SIA	Security impact analysis	This family does not apply to an initial evaluation.

5.3 CORRECT ASSURANCES

5.3.1 Dependencies for assurances

Table 5.3.1-1 shows correctness of the assurances with respect to meeting all dependencies.

Table 5.3.1-1 Correct Assurances – Dependency Mapping

Item #	Component	Component Title	Dependency	Item #
1	ACM_CAP.3	Authorization controls	ACM_SCP.1 ALC_DVS.1	2* 11
2	ACM_SCP.2	Problem tracking CM Coverage	ACM_CAP.3	1
3	ADO_DEL.1	Delivery procedures	—	—
4	ADO_IGS.1	Installation, Generation, and Start-up Procedures	AGD_ADM.1	9
5	ADV_FSP.1	Informal functional specification	ADV_RCR.1	7
6	ADV_HLD.1	Descriptive High-Level Design	ADV_FSP.1 ADV_RCR.1	5 7
7	ADV_RCR.1	Informal Correspondence Demonstration	—	—
8	ADV_SPM.1	Informal TOE security policy model	ADV_FSP.1	5
9	AGD_ADM.1	Administrator Guidance	ADV_FSP.1	5
10	AGD_USR.1	User Guidance	ADV_FSP.1	5
11	ALC_DVS.1	Identification of Security Measures	—	—
12	ALC_FLR.2	Flaw reporting procedures	—	—
13	ATE_COV.2	Analysis of coverage	ADV_FSP.1 ATE_FUN.1	5 15
14	ATE_DPT.1	Testing: High-Level Design	ADV_HLD.1 ATE_FUN.1	6 15
15	ATE_FUN.1	Functional Testing	—	—
16	ATE_IND.2	Independent Testing - Sample	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1	5 9 10 15
17	AVA_MSU.2	Validation of analysis	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1	4 5 9 10
18	AVA_SOF.1	Strength of TOE Security Function Evaluation	ADV_FSP.1 ADV_HLD.1	5 6
19	AVA_VLA.1	Developer vulnerability Analysis	ADV_FSP.1 ADV_HLD.1 AGD_ADM.1 AGD_USR.1	5 6 9 10

* - indicates that this dependency is covered by a strictly hierarchical component

5.3.2 Assurance Operations

There are no operations performed on assurance components in CSPP.

A. APPENDIX A - REFERENCES

[CC-V2.1] *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999.

[CSPP] *CSPP - Guidance for COTS Security Protection Profiles*, December 1999.