National Nuclear Security Administration

Policy Letter: NAP-14.3

Date: September 12, 2003

TITLE: NNSA Protection Profile and Security Target Requirements

1. INTRODUCTION. This NAP identifies the requirements and process for developing cyber security Protection Profiles (PPs) and Security Targets (STs) that will contain the cyber security functional and assurance requirements used to protect information on NNSA information systems. This process integrates the NNSA Program Secretarial Office Cyber Security Program (PCSP), the NNSA Cyber Threat Statement, and the International Standard ISO IS 15408, *Common Criteria*, *Version 2.1,* methods and criteria to the identification and documentation in PPs and STs of cyber security functional and assurance requirements for information systems.

2. OBJECTIVE. Establish requirements for development of PPs and STs for the protection of information and NNSA information systems

3. APPLICABILITY. This NNSA Policy (NAP) applies to all entities, Federal or contractor, that develop PPs or STs for information systems that collect, create, process, transmit, store, and disseminate information for NNSA.

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

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

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

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

   e. SCI Exclusion. These requirements do not apply to systems processing sensitive compartmented information (SCI). SCI must be protected in accordance with the appropriate intelligence community policies and directives.

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

5. REQUIREMENTS.

   a. All PPs and STs for NNSA information and information systems must be developed and approved in accordance with the requirements and process in this NAP.

   b. The development of a PP or ST that will contain the cyber security functional and assurance requirements used to protect information on NNSA information systems must integrate the NNSA Program Secretarial Office Cyber Security Program (PCSP), the NNSA Cyber Threat Statement, and the International Standard ISO IS 15408, *Common Criteria*, *Version 2.1,* methods and criteria to identify and document the cyber security functional and assurance requirements for NNSA information and information systems.

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

7. DEFINITIONS. See Attachment 2.

BY ORDER OF THE ADMINISTRATOR:

Linton Brooks
Administrator

Attachments

CHAPTER I

PROTECTION PROFILES AND SECURITY TARGETS

1. Protection Profiles. All cyber security protection measures for all NNSA information must be documented in approved PPs. A PP is an implementation independent statement of security requirements that is shown to address threats that exist in a specified environment. NNSA PPs are used to specify cyber security requirements for information groups defined in the NNSA PCSP. The protection requirements for a unique situation, such as, information requiring special protection or a collection of information groups that require special protection because of the aggregation, must be documented in a PP and approved by NNSA.

    a. PP Contents. An NNSA PP is based on the definition of a PP in the International Standard 15408, *Common Criteria, Part 1, Annex B,* and must contain the following sections

        (1) PP Introduction

            (a) PP identification

            (b) PP overview

        (2) Information System (TOE) Description

        (3) TOE Security Environment

            (a) Assumptions

            (b) Threats

            (c) Organizational security policies

        (4) Security Objectives

            (a) Security objectives for the information system

            (b) Security objectives for the information system environment

        (5) Information System Security Requirements

            (a) Information System Security Requirements

                i. Security functional requirements

                ii. Security assurance requirements

            (b) Security requirements for the information system environment

(6) PP Application notes

(7) Rationale

(a) Security Objectives Rationale

(b) Security Requirements Rationale

8. Security Targets. All cyber security protection measures for all NNSA information systems must be documented in approved STs. An ST describes how a specific information system implements the cyber security requirements in a PP. The ST contains the information system security threats, objectives, requirements, and summary specification of security functions and assurance measures.

a. ST Contents. An NNSA ST is based on an approved NNSA PP and the definition of an ST in the International Standard 15408, *Common Criteria, Part 1, Annex C*. An NNSA ST must contain the following sections.

(1) ST Introduction

(a) ST identification

(b) ST overview

(c) PCSP conformance

(2) Information System Description

(3) Information System Security Environment

(a) Assumptions

(b) Threats

(c) Organizational security policies

(4) Security Objectives

(a) Security objectives for the information system

(b) Security objectives for the environment

(5) Information System Security Requirements

(a) Information System Security Requirements

i. TOE security functional requirements

ii. TOE security assurance requirements

(b) Security requirements for the information system environment

(6) Information System Summary Specification

(a) TOE security functions

(b) Assurance measures

(7) PP Claims

(a) PP reference

(b) PP refinement

(c) PP additions

(8) Rationale

(a) Security objectives rationale

(b) Security requirements rationale

(c) TOE summary specification rationale

(d) PP claims rationale

9. Guide to Writing PPs and STs. NNSA has adapted the Common Criteria (CC) documentation and process for the construction of Protection Profiles (PPs) and Security Targets (STs). CC documentation for the construction of PPs and STs is primarily aimed at those who are involved in the development of PPs and STs. However, the documentation may also be useful in the development, review, and analysis of the System Security Plan required for every NNSA information system.

10. Constructing Protection Profiles. The PP provides a framework within which to specify security requirements. The steps (Figure 1) are:

a. Describe the environment in which the information system will reside. Determine the information groups on the information system. Identify any unique or local threats against the information or the information system. Identify any assumptions made about the local environment. Identify any NNSA or element policies to which the information system must conform.

b. Based on the requirements in the NNSA PCSP, identify the functionality protection objectives (Attachment 3) that must be met for all information groups on the information system. NOTE: The functionality protection objectives (in Attachment 3) in this NAP integrate the NNSA Cyber Security Threat Assessment and NNSA cyber security policies and are the minimum objectives for each information group that must be addressed in the PP. Develop any additional objectives required to address element policies, local threats, and

assumptions. The objectives should not be simply a negation of the threat, and should be realistic and achievable. The objectives should be separated into those that are to be achieved by the information system, those that are to be achieved in the environment (information system or otherwise), and those that are to be achieved by a combination of the two.

c. Use the CC Part 2 security functional requirements catalogue to identify the security functional components that will support each objective identified for the system and each objective for other information technology within the environment. Additional security functional requirements can be added to a functional component when needed to meet additional objectives or requirements. Identification of functional components should be completed where there is a need to be more specific than the generalized requirement in CC Part 2. Where appropriate components cannot be identified from Part 2, new ones may be devised in a similar format.

d. Based on Chapter III, identify the assurance level (AL) and assurance components (Attachment 4) required by the information groups on the information system.

e. The final step is to provide a rationale that shows how the selected functional and assurance components are suitable to satisfy the cyber security objectives.

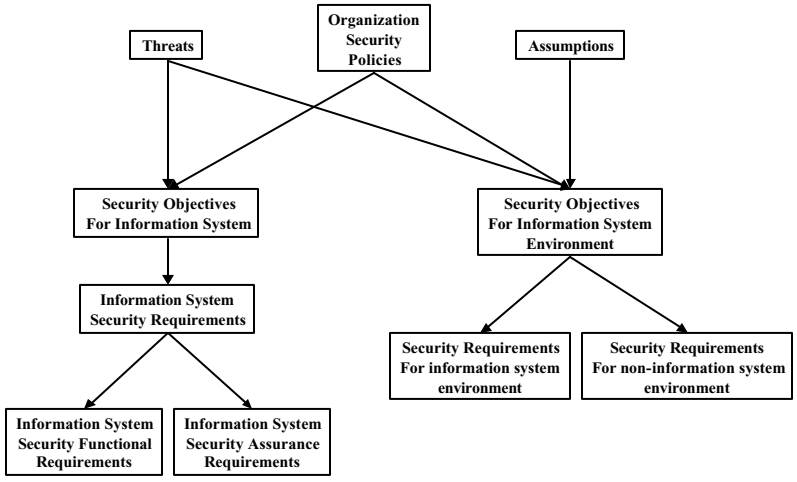


Figure 1. Constructing Protection Profiles

11. Building On Existing Work[1]. The CC model is founded on the principles of modularity and reuse. The CC functional and assurance requirements catalogues were provided with this end in mind. It is intended that users should take advantage of the efforts of others when using the CC and this approach is well illustrated by the process of system specification.

[1] When reusing Protection Profiles, care should be taken to avoid any infringement of copyright.

In the simplest case an existing PP may be found that addresses the entire requirement. It may be that two or more existing PPs are needed to meet requirements. This case is almost as straightforward, although it will be necessary to demonstrate that the PPs are consistent and do not conflict.

Failing this, it may be possible to take an existing PP, and adapt it to meet modified requirements. This modification may take the form of a change to the intended environment (threats, assumptions, organizational security policies), with the results of:

- Inserted or deleted functional requirements
- Inserted or deleted assurance requirements
- Modified completion of operations

It is in the process of modifying an existing PP that the benefits of the rationale become evident. Through examination of the rationale, the impact on satisfaction of objectives of any change in the functional requirements can be determined. Similarly, if an objective is no longer required it can be seen which requirements can safely be removed.

It may be that more than one PP is required to address the overall requirement. These PPs may be used in their entirety, or may be modified to suit. In the former case, a PP may claim conformance to one or more existing PPs (e.g. operating system PP, database PP, secure data exchange PP). In the latter, it may be necessary to modify the content of a PP, in which case it may no longer be possible to claim conformance. In all cases, it will need to be shown that the incorporated material is consistent, and meets the objectives of the overall PP.

A PP adapted from an existing PP must be reviewed and approved by NNSA.

12. Specifying A System Based On CC Evaluated Products. Existing product specifications (STs) developed by a product vendor or another organization can assist in the preparation of a PP. The advantage of this approach is that it should be much easier to address the resulting system specification from available certified/validated products.

    A suggested method is to begin by identifying the security environment for the system (information groups, threats, assumptions and organizational security policies) and to derive a set of objectives. A review of security targets should then be conducted to identify similar objectives. The related security requirements can then be drawn out (using the rationales) and assembled into a PP. An iterative approach should be adopted, trying out various products or combinations of products, to find the best match and reassessing risk each time. It should be considered whether moving objectives from information system to environment might provide a more cost-effective solution for any objectives not met by an existing product, substituting procedural measures for IT.

It may thus be possible to construct a system ST that, both, meets the system objectives and can be implemented using evaluated products.

CHAPTER II

FUNCTIONALITY PROTECTION OBJECTIVES

1. Introduction. This chapter describes the methodology for selecting a set of functionality components based upon the threat and the information group(s) on an information system.

   The functionality protection objectives listed in Attachment 3 have been assigned by NNSA using the Consequence of Loss levels listed in Table 4, NAP-14.1, *NNSA Cyber Security Program,* and the NNSA Cyber Threat Assessment. The objectives listed for each information group are the minimum set of functionality protection objectives that must be addressed by the Information Groups PPs and information system's ST.

2. Determining Functionality Protection Objectives. This section identifies the process for identifying functionality protection objectives. Figure 2 presents a flow diagram of the PP selection process.

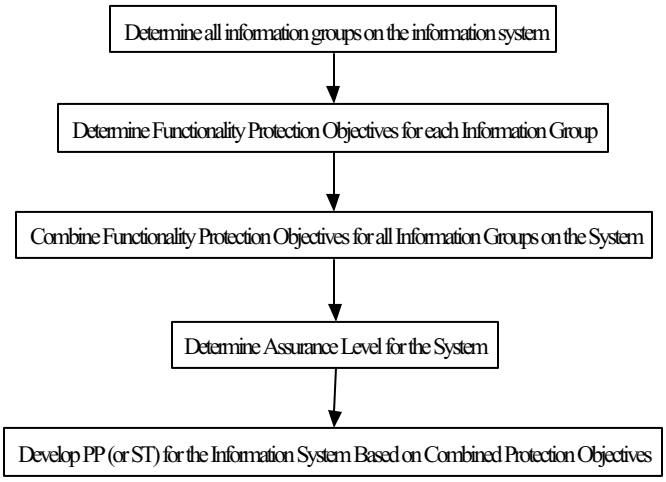


Figure 2. Determination of Protection Objectives

   a. Information Groups. The initial step of the process is to identify all the Information Groups that will be placed on the information system and establish the confidentiality, integrity, and availability Consequence of Loss requirements for each information group.

   b. Determine Protection Objectives. For each information group to be placed on the system, identify the functionality protection objectives, using the table in Attachment 4. If the Consequence of Loss of confidentiality, integrity, or availability exceeds the minimums established for an Information Group (i.e., if

they exceed the minimums established in Table 4, NAP-14.1, *NNSA Cyber Security Program,* and the NNSA Cyber Threat Assessment) then, the minimum functionality protection objectives are adjusted. To adjust an objective, review Attachment 3 to see if adjacent or other predefined objectives will meet the expanded or additional security requirements or higher Consequence of Loss requirement. Additional functionality protection objectives may be developed to address the expanded or additional requirements, following the process defined in Chapter I, Section 10.

c. Combine Protection Objectives. After the functionality protection objectives for each information group have been determined, combine the list of protection objectives for all information groups on the system into a single set of objectives.

d. Assurance Level. For each information group to be placed on the system, determine the Assurance Level, using Chapter III, Table 1. If the Consequence of Loss of confidentiality, integrity, or availability exceeds the minimums established for an Information Group (i.e., if they exceed the minimums established in Table 4, NAP-14.1, *NNSA Cyber Security Program,* and the NNSA Cyber Threat Assessment) then, the minimum assurance components are adjusted to address the expanded or additional requirements.

e. Develop Protection Profiles and Security Targets. This list of functionality protection objectives and the Assurance Level is used to develop a PP or ST for the information system. The development of a PP or ST includes the selection of functional and assurance components from the CC Part 2 and Part 3 that achieve the protection objectives and Assurance Level.

3. Protection Profile and Security Target Requirements. This section defines the requirements for the generation of PPs and ST. Figure 3 shows the possible approaches to developing a Security Target.

a. Protection Profile and Security Target Requirements. The following general requirements apply to the generation of PPs and STs:

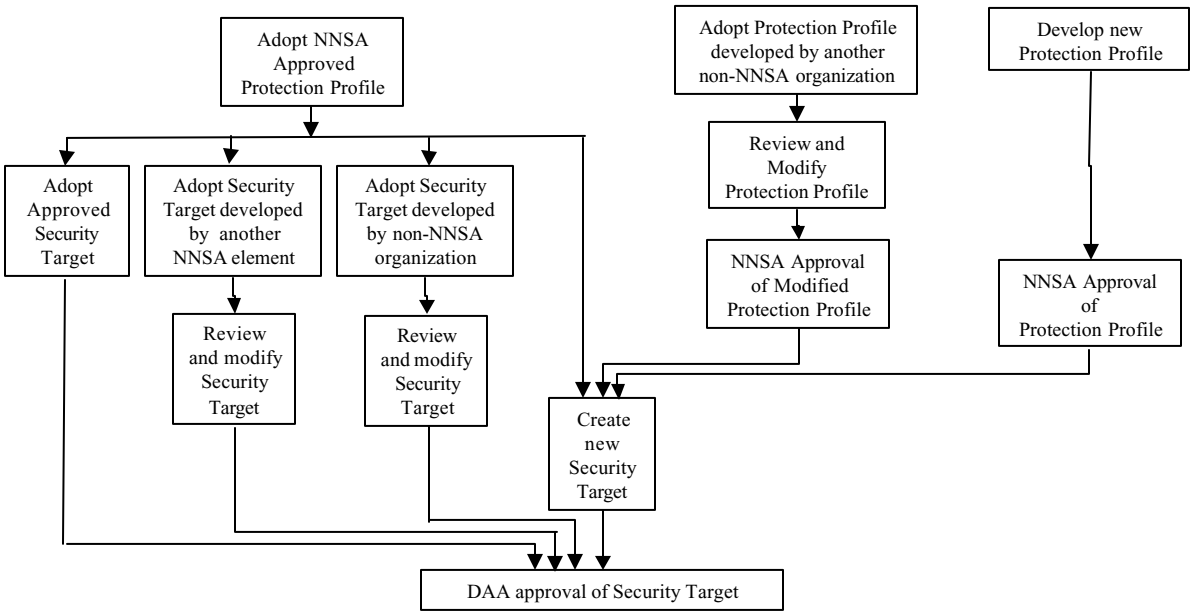
(1) Every Security Plan will be supported by at least one PP and at least one ST.

(2) Every ST will be based upon at least one PP

(3) Every component of the information system must be addressed in a ST.

(4) All PPs must be approved by the NNSA CSPM.

(5) The DAA reviews STs for conformance with the PP and the information system Security Plan and approves the ST for implementation.



b. PP/ST Functionality and Assurance Components. The protection objectives in Attachment 2 and the assurance components in Attachment 4 are used to determine the minimum Common Criteria and NNSA functionality and assurance components that are included in the PP or ST. The objectives or the components derived from the objectives may be adjusted or new components added if:

(1) The data owner or data steward for information within an information group on the information system has expanded or required additional confidentiality, integrity, or availability protection requirements for the information group. If the DAA concurs with these requirements, the minimum functionality and assurance components are adjusted to address the expanded or additional requirements. Note: These adjustments must also be documented in the Security Plan.

(2) The DAA for the information system has expanded or required additional confidentiality, integrity, or availability protection requirements for the information system. The minimum functionality and assurance components are adjusted to address the expanded or additional requirements. Note: These adjustments must also be documented in the Security Plan.

c. Protection Profile and Security Target Generation. All approved PPs must be registered in the NNSA PP Library maintained by the NSSA CSPM. Figure 3, above, identifies three possible approaches: Using a NNSA approved PP; adopting a PP developed by a non-NNSA organization, and developing a new PP. The processes are described in the following sections.

(1) NNSA Approved Protection Profile. If an NNSA approved PP is selected, and:

(a) If an NNSA-approved ST that supports the approved PP is selected, the PP and ST are incorporated into the information system Security Plan and the ST will be approved as part of the accreditation process.

If an ST that supports the approved PP but has been developed for another NNSA information system is selected, the ST must reviewed, and modified as needed, to ensure any adjustments to the protection objectives or site specific changes have been incorporated. After ST review and approval by the cognizant DAA, the ST is incorporated into the information system Security Plan.

(b) If an ST that supports the approved PP but has been developed for a non-NNSA information system is selected, the ST must reviewed, and modified as needed, to ensure any adjustments to the protection objectives or site specific changes have been incorporated. After ST review and approval by the cognizant DAA, the ST is incorporated into the information system Security Plan.

(c) If a new ST must be developed, the NNSA approved PP is the basis for the ST. After ST review and approval by the cognizant DAA, the ST is incorporated into the information system Security Plan.

(2) Adopt A Protection Profile from A Non-NNSA Organization. The PP must be reviewed and modified to ensure that the selected (and possibly adjusted) protection objective functionality and assurance components have been incorporated. Once the PP has been developed it must be approved by the NNSA CSPM to ensure consistency and registered in the NNSA PP Library. Once the modified PP has been approved, a new ST must be developed as described above. After ST is reviewed and approved by the cognizant DAA, the ST can be incorporated into the information system Security Plan.

(3) Develop New Protection Profile. The PP must be developed following NNSA PP development guidelines. The PP must be approved by the NNSA CSPM to ensure consistency and registered in the NNSA PP Library. Once the new PP is approved, an ST must be developed as described in paragraph 3.c.(1)(c) above. After the ST is reviewed and approved by the cognizant DAA, the ST is incorporated into the information system Security Plan.

CHAPTER III

ASSURANCE LEVELS

1. Introduction. This chapter describes the methodology for selecting a set of assurance components based upon the highest Consequence of Loss of confidentiality and integrity for all information groups on the information system. The selected set of assurance components represents the minimum set of components that must be applied to the information system.

   The Assurance components are used to provide a level of confidence (assurance) that the information system meets its security objectives. This level of confidence is graded by an Assurance Level that is based on the consequence of loss for confidentiality or integrity, whichever is higher.

2. Determining Assurance Level. This section identifies the process for identifying the Assurance Level for an information system.

   a. Information Groups. The initial step of the process identifies all of the information groups that will be placed on the information system and establish the confidentiality and availability Consequence of Loss for each information group.

   b. Determine Assurance Level. Determine the highest Consequence of Loss for confidentiality and integrity for all information groups on the system. Using this highest level of consequence identify the assurance level from the following table. Even if the Consequence of Loss of confidentiality or integrity requirements exceed the minimums established for an Information Group (i.e., if they exceed the minimums established in Table 4, NAP-14.1, *NNSA Cyber Security Program,* and the NNSA Cyber Threat Assessment) the minimum assurance level will be based on the highest Consequence of Loss.

Table 1. Assurance Level

Highest Consequence of Loss for Confidentiality or Integrity	Assurance Level
Very Low	0 - Scope and content negotiated between DAA and system owner
Low	1 - Functional
Medium	2 - Structurally Tested
High	3 - Methodically Tested and Checked
Very High	4 - Methodically designed, tested, and reviewed

   c. Identify the Assurance Level Components. From Attachment 4 identify the assurance components needed to support the identified assurance level. If additional assurance requirements are needed for the selected assurance level,

additional elements may be added to any of the assurance components or additional assurance components may be selected from those identified in CC Part 3. Where appropriate security functional components cannot be identified from Part 3, new ones may be devised in a similar format following the process defined in Chapter I, Section 10. Note: These adjustments must also be documented in the Security Plan.

d. Identify the Maintenance of Assurance components. From Attachment 4 also identify the Maintenance of Assurance components needed to support the identified Consequence of Loss level. The Maintenance of Assurance components are also based on the highest Consequence of Loss determined in paragraph 2.b. above. If additional Maintenance of Assurance requirements are needed for the selected Consequence of Loss level, additional elements may be added to any of the Maintenance of Assurance components or additional components may be selected from those identified in CC Part 3. Where appropriate security functional components cannot be identified from Part 3, new ones may be devised in a similar format following the process defined in Chapter I, Section 10. Note: These adjustments must also be documented in the Security Plan.

ATTACHMENT 1

DEFINITIONS

Data Owner	The person responsible for having information reviewed for sensitivity and classification. This person is responsible for its generation, management, and destruction.
Data Steward	The person acting on behalf of the data owner for the generation, management, and destruction of data and to ensure the review of information sensitivity and classification.
Formal Access Approval	Access to information is authorized in writing with justification. Documented approval by a data owner or data steward to allow access to information (e.g. A clearance provides formal access approval to a level and category of information). Formal assignment to process personnel or health records is documented evidence of formal access approval to unclassified Privacy Act information.)
Protection Profile (PP)	An implementation-independent set of security requirements for information systems that are used to support a specific information group.
Security Function (SF)	Part or parts of the information system that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
Security Function Policy (SFP)	The security policy enforced by an SF.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation (certification) of an information system
Target of Evaluation (TOE)	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected and distributed within a TOE.

ATTACHMENT 2

FUNCTIONALITY PROTECTION OBJECTIVES

Table 2

Objective Name	Objective Description
O.ACCESS	Each user's access rights and privileges are authorized, prior to the user's first access to the TOE.
O.ACCESS_AUTH_L	All users (including privileged users) shall, at a minimum, possess a current "L" Access Authorization prior to their first access to the TOE
O.ACCESS_AUTH_Q	All users (including privileged users) shall possess, at a minimum, a current "Q" Access Authorization prior to their first access to the TOE
O.ACCESS_FORMAL	Prior to their first access to information, each user's need-to-know is formally authorized by management or the data owner-steward through a position description or written access list.
O.ACCESS_HISTORY	The information system user is notified upon successful logon of a) the date and time of the user's last logon, b) the location of the user (as can best be determined) at last logon, and c) the number of unsuccessful logon attempts using this user ID since the last successful logon. A positive action by the user is required to remove the notice.
O.ACCESS_MALICIOUS	Environmental controls are required to sufficiently mitigate (deterrence, detection, and response) the threat of malicious actions by authenticated users. Information system controls will help in achieving this objective, but will not be sufficient.
O.ALT_POWER_SUPPLY	Transfer of the system to another power source is completed within the time requirements of the application(s).
O.AUDIT_AUTOMATED_REVIEW	Audit analysis and reporting of auditable events using automated tools must be scheduled and performed.
O.AUDIT_BASIC	The following activities must be recorded: • Successful use of the user security attribute administration functions; • All attempted uses of the user security attribute administration functions; and • Identification of which user security attributes have been modified. • With the exception of specific sensitive attribute data items (e.g., passwords, cryptographic keys), new values of the attributes should be captured. • Successful & unsuccessful logons and logoffs; • Successful and unsuccessful access to security relevant files including creating, opening, closing, modifying, & deleting those files; • Changes in user authenticators; • Blocking or blacklisting user IDs, terminals, or access ports; • Denial of access for excessive logon attempts; and • Starting and ending times for each access to the system
O.AUDIT_CONTINOUS_MONITORING	Auditing must include the continuous, online monitoring of auditable events. The system must notify an authorized person when imminent violations of security policies are detected.

Objective Name	Objective Description
O.AUDIT_FAILURE	An alternate audit capability or system shutdown must occur in the event of audit failure or when the audit trail exceeds 80% of capacity.
O.AUDIT_PROTECTION	The contents of audit trails must be protected against unauthorized access, modification, or deletion.
O.AUDIT_REVIEW	There must be a process for review of user activities and activities on behalf of the user on the TOE to detect and report actual or attempted circumvention of the TOE Security Functions (TSF).
O.AUDIT_SELECTED_EVENTS	The audit trail must include records of– (a) Privileged activities at the system console (either physical or logical consoles) and other system- level accesses by privileged users and (b) The creation, deletion, or changes in security labels.
O.AUTHENT_EXPOSE	The clear text display or exposure of any authenticator is only provided to the identified user during generation, issuance, storage, or use.
O.AUTHORIZATION	The TOE must ensure that only authorized users gain access to the information and TOE resources. The TOE must ensure for all actions under its control, except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access to subjects and objects.
O.AUTHORIZE_NON_TOE:	The IT other than the information system must provide the ability to specify and manage user and system process access rights to individual processing resources and data elements under its control, supporting the organization's security policy for access control.
O.AVAILABILITY_HIGH	The information system provides near-continuous processing even with critical component failure.
O.AVAILABILITY_LOW	Resources are provided to allow the information system user to perform data backup at the users discretion.
O.AVAILABILITY_MEDIUM	System backup and contingency hardware is identified for critical component replacement to processing applications. Operations are resumed within a time period to ensure the security of the site and health and safety of employees and the public.
O.BACKUP_ESSENTIAL	Complete restoration of information from backup media must be tested periodically.
O.CLEARING	The information system components and removable media are cleared before the items can be reused in another system environment with the same or lower accreditation level as the original system components or removable media.
O.COVERT_CHANNEL_REMOVE	Covert channels with a bandwidth greater than 1,000 bytes per second must be eliminated or DAA acceptance of risk obtained for each covert channel not eliminated.
O.COVERT_CHANNEL_REVIEW	The information system must be reviewed to identify obvious covert channels with a bandwidth greater than 1,000 bytes per second
O.CREDENTIAL_PROTECTION	Authentication credentials shall be protected from unauthorized access, modification, deletion, of destruction.
O.CTL_IF_FAILSECUR	All possible failures of a controlled interface result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability.
O.CTL_IF_PLATFORM	The controlled interface (CI) meets the protection requirements for the information group with the highest consequence of loss for confidentiality, integrity, and availability on all information systems connected to the CI. For example, if a CI connects to an information system with a consequence of loss of "High" and another information system with a consequence of loss of "Low", the CI must meet the protection and assurance requirements for the information group with the "High" consequence of loss.

Objective Name	Objective Description
O.CTL_IF_ROUTING	The controlled interface bases its routing decisions on information that is supplied or alterable only by the controlled interface security functions
O.CTL_IF_USR_CODE	The controlled interface does not run any general user code.
O.CTL_IF_FAILSECURE	All possible failures of the controlled interface result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability
O.CTL_IF_POLICIES	Communication policies and connections that are not explicitly permitted are prohibited
O.CTL_INTERFACE	Protection requirements and adjudication of security policy differences are enforced when two or more information systems or networks are interconnected
O.DATA_BACKUP_BASIC	User and information system data are available, or restorable, to meet mission availability requirements. Periodic checking of backup inventory and testing of the ability to restore information is accomplished to validate mission availability requirements are met.
O.DATA_BACKUP_EXTENDED	Media containing backup files and backup documentation must be stored at another location, such as a nearby building or off site, to reduce the possibility of the loss of backup data. Backup procedures must be verified periodically by confirming that the date of last backup is consistent with the backup procedures.
O.DATA_CHANGES_DETECTED	Unauthorized changes to data in the information system are detected and reported.
O.DATA_CHANGES_DETERRED	Unauthorized changes to data in the information system are detected, deterred, and reported.
O.DATA_CHANGES_PREVENTED	Unauthorized changes to data in the information system are prevented and reported; or unauthorized changes are immediately corrected and reported.
O.DETECT_EXTERNAL_BASIC	The site environment, i.e., on-line, must provide the ability to detect low level, i.e., using methods readily available on the Internet to attack known vulnerabilities, attacks on the hosts and networks from outside the site and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.
O.DETECT_EXTERNAL_SOPHISTICATED	The site environment, i.e., on-line, must provide the ability to detect sophisticated attacks on the hosts and networks from outside the site and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.
O.DETECT_HOST_BASIC	The information system environment, i.e., on-line, must provide the ability to detect low level, i.e., using methods readily available on the Internet to attack known vulnerabilities, attacks and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.
O.DETECT_HOST_SOPHISTICATED	The information system environment, i.e., on-line, must provide the ability to detect sophisticated attacks and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.
O.DETECT_NETWORK_BASIC	The network environment, i.e., on-line, must provide the ability to detect low level, i.e., using methods readily available on the Internet to attack known vulnerabilities, attacks on the network and its components, and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.
O.DETECT_NETWORK_SOPHISTICATED	The network environment, i.e., on-line, must provide the ability to detect sophisticated attacks on the network and its components, and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.

Objective Name	Objective Description
O.DETECT_SITE_BASIC	The site physical environment must provide the ability to detect low level, i.e., using readily available methods to attack known vulnerabilities, attacks on the hosts and networks from inside the site and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.
O.DETECT_SITE_SOPHISTICATED	The site physical environment must provide the ability to detect sophisticated attacks on the hosts and networks from inside the site and the results of such attacks (e.g., corrupted system state), including measures to detect and respond to unauthorized attempts to penetrate or deny use.
O.ENTRY_NON_TECHNICAL	The information system environment must provide sufficient protection against non-technical attacks by other than authenticated users. User training and awareness will provide a major part of achieving this objective.
O.ENTRY_NON_TOE	For resources not controlled by the information system, IT other than the information system must prevent logical entry using unsophisticated, technical methods, by persons without authority for such access.
O.ENTRY_TOE	The information system must prevent logical entry to the information system using unsophisticated, technical methods, by persons without authority for such access.
O.FAIL_SECURE	The information system shall enter a secure state such that information flows are disabled upon detection of any condition that prevents it from continuing to operate securely.
O.FORENSICS_PROC	Procedures are established and documented to ensure the identification, collection, and preservation of data needed to analyze penetration reconstruction, on-going cyber attacks and/ or failures
O.FULL_RESIDUAL_PROTECTION	The information system must ensure that all resources contain no residual data before being assigned, allocated, or reallocated.
O.HARDWARE_EXAM_BASIC	Information system hardware components are examined for security impacts to the information system before use. . In addition, the hardware review will validate the chip sets and boards are from the manufacturer
O.HARDWARE_EXAM_COMPREHENSIVE	Information system hardware components are examined for security impacts to the information system before use. In addition, the hardware review will validate the chip sets and boards are from the manufacturer and using the manufacturer diagnostics confirm the information system chip sets and boards function as expected.
O.HARDWARE_EXAM_MINIMUM	Information system hardware components are examined for security impacts t o the information system before use
O.ID_DISABLE	User TOE access is disabled when the user leaves the sponsoring organization, Access Authorization is terminated, loses authorized access (for cause, changes in organization, etc), or upon TOE detection of attempts to bypass security.
O.ID_REMOVAL	Prior to reuse of a user identifier, all previous access rights and privileges (including file accesses for that user identifier) are removed from the TOE
O.ID_REVALIDATION	User access, contact information, rights, and privileges, to include sponsor, Access Authorization, need-to-know, means for off line contact, mailing address, are validated annually.
O.INFO_FLOW	The information system and information system environment must ensure that any information flow control policies are enforced - (1) between system components and (2) at the system external interfaces.
O.INTEGRITY_HIGH	The TOE will require identification and authentication to validate the authority of the user to make changes; and maintain a log that identifies the user that attempted to change or actually changed data, and correlates the user with the data. The TOE shall immediately disable the userID of a user that attempts an unauthorized change.
O.INTEGRITY_LOW	The TOE will validate the authority of the user for any changes to data.

Objective Name	Objective Description
O.INTEGRITY_MEDIUM	The TOE will require identification and authentication to validate the authority of the user to make changes; and maintain a log that identifies the user that attempted to change or actually changed data, and correlates the user with the data
O.INTEGRITY_VERY_HIGH	The TOE will require identification and authentication to validate the authority of the user to make changes; and maintain a log that identifies the user that attempted to change or actually changed data, and correlates the user with the data. The TOE shall immediately disable the userID of a user that attempts an unauthorized change and notify personnel responsible for TOE security.
O.MALICIOUS_CODE	The TOE must have the capability to detect and eliminate malicious code. Procedures to detect and deter incidents caused by malicious code are employed.
O.MANAGE_TOE	The information system must provide all the functions and facilities necessary to support the administrators that are responsible for the management of information system security.
O.MARK_COMPONENT	Each host, visual display, and output device will be marked with the sensitivity label (level) of the most sensitive information group the system is accredited to process, store, or transmit.
O.MARK_OUTPUT	All system output and removable media are appropriately marked with the level of the highest information sensitivity of the information groups the system is accredited to operate with, or marked in with the sensitivity label for the information.
O.MEDIA_REVIEW	All media (paper, disks, zip drives, removable disk drives, etc.) are reviewed for classification and sensitivity and properly marked before release outside the system boundary.
O.NETWORK_INTERFACE	The developers of the information system must ensure the information system security is not adversely affected by the characteristics of the network(s) to which the information system is interfaced.
O.NTK_NNSA	Access rights to specific data objects are determined by object attributes assigned to that object, user identity, user attributes, and any formal access rights or privileges that NNSA has established for the data.
O.ORIGIN_PROOF	A subject receiving information during a data exchange is provided evidence of the origin of the information.
O.PHY_CLASSIFIED	Systems containing classified Top Secret (TS) information may be protected in one of the following ways: constantly attended or under the control of a person that possesses proper Access Authorization, formal access approval, and need to know; in a locked General Services Administration (GSA) approved security container with supplemental controls; or in a vault or vault-type room. Specific criteria are defined in DOE orders. Systems containing classified Secret information shall be protected in one of the following ways: constantly attended or under the control of a person that possesses proper Access Authorization, formal access approval, and need to know, in a locked GSA approved container; or in a vault or vault-type room. Systems containing classified Confidential information shall be stored in manner authorized for Secret or a GSA approved security container.
O.PHY_PROT_UNCLASSIFIED	Systems containing Unclassified Protected information shall, as a minimum, be protected in one of the following ways: constantly attended or under the control of a person that possesses formal access approval and need to know; in a manner described for Unclassified Mandatory Protection information; or in a manner to preclude unauthorized disclosure.
O.PHYS_MANDATED	Systems containing Unclassified Mandatory Protection information must be protected in one of the following ways: constantly attended or under the control of a person that possesses formal access approval and need to know; or protected in a manner described for Confidential or Critical Unclassified Information; or protected within locked rooms or buildings.
O.PHYSICAL	Physical attack that might compromise IT security on those parts of the information system critical to security is deterred and detected, primarily via prevention within the limits of COTS technology.

Objective Name	Objective Description
O.PHYSICAL_PROTECTION	The individuals responsible for the information system must ensure that the environment is capable of physically protecting the information system by signaling the occurrence of fire, flood, power loss, and environmental control failures that might adversely affect information system operations.
O.RECEIPT_PROOF	A subject transmitting information during a data exchange is provided evidence of the receipt of the information.
O.RECOVERY_CONTROLLED	Information system recovery is controlled via monitored terminal or system console.
O.RECOVERY_SECURE	Information system recovery occurs in a secure, trusted manner.
O.REPLAY	The information system must detect and deter replay of entities, such as messages and service requests and responses.
O.RESIDUAL_PROTECTION	The information system must ensure that identified resources contain no residual data before being assigned, allocated, or reallocated.
O.RESOURCE_USAGE	The information system provides the capability to control a defined set of system resources (e. g., memory, disk space) such that no one user can deny another user access to the resources.
O.ROLE_SYS_ADM_&_ISSO	The same person does not perform the functions of the ISSO and the system administrator.
O.ROLES_OTHER_SECURITY	Other roles involved with security administration, such as DBMS administration, are not performed by the same people performing the ISSO and system administrator roles.
O.ROLES_TWO_PERSON	The ISSO and system administrator are present when audit parameters or audit file contents are modified.
O.SANITIZATION	All information system components and removable media are sanitized, using approved NNSA procedures, prior to release for use at a lower classification level, at a lower level of consequence, or outside the information system boundary.
O.SEC_FUNC_MANAGEMENT	The information system restricts management of information system security functions to authenticated users.
O.SECURITY_LEVEL_CHANGES	The information system must immediately notify the user of each change in the security level or compartment associated with that user during an interactive session. A user must be able to query the information system as desired for a display of the user's complete sensitivity label.
O.SESSION_ESTABLISHMENT	The information system controls the establishment of sessions (a) by denying access after multiple (maximum of three) consecutive unsuccessful attempts on the same user ID; (b) by limiting the number of access attempts in a specified time period, (c) by use of a time-delay control system, or (d) by other such methods, subject to approval by the DAA
O.SOFTWARE_EXAM_BASIC	Software is examined to determine if the software conforms to the security relevant controls as documented by the developer and contains no malicious code.
O.SOFTWARE_EXAM_COMPREHENSIVE	Software is examined to determine if the software conforms to the security relevant controls as documented by the developer. The examination will also determine if the controls can be bypassed or subverted
O.SOFTWARE_EXAM_MINIMUM	Information system software components are examined and tested for security impacts to the information system before use.
O.SUBJECT_DOMAIN_SEPARATION	The information system enforces domain separation for all information system subjects.
O.TRAINING	All users are trained to understand applicable information system-use policies, the approved use of the information system, the vulnerabilities inherent in the operation of the information system, and their cyber security responsibilities.

Objective Name	Objective Description
O.TRANS_SEC_CLASS	Information protection is required whenever classified information is to be transmitted, carried to, or carried through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e. g., outside the system perimeter). One or more of the following must be used: (a) Information distributed only within an area approved for open storage of the information; (b) National Security Agency (NSA)- approved encryption mechanisms appropriate for the encryption of classified information; (c) Protected Transmission System; and (d) Trusted courier.
O.TRANS_SEC_UNCLASS	Information protection is required whenever information is to be transmitted, carried to, or carried through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e. g., outside the system perimeter).
O.TRUSTED_PATH	The information system provides a trusted path between itself and the user for initial identification and authentication.
O.TRUSTED_PATH_COMMO	The information system provides a trusted path between itself and the user for all communications between the information system and the user.
O.TSF_DOMAIN_SEPARATION	The information system maintains a domain for its own execution that protects it from external interference and tampering (e. g., by reading or modifying its code and data structures).
O.UNESCORT_ACCESS_CLASSIFIED	Access controls ensure that personnel granted unescorted physical access to information, the information system or human readable media, have the appropriate security clearance, formal access approvals and need-to-know.
O.UNESCORT_ACCESS_UNCLASS	Access controls ensure that personnel granted unescorted physical access to the information, the information system or human readable media have the appropriate formal access approvals and need-to-know.
O.USER_INACTIVITY	The information system must detect an interval of user inactivity, such as no keyboard entries, and disable any future user activity until the user reestablishes the correct identity with a valid authenticator.
O.USER_LOCKING	The information system provides user initiated self-locking of interactive sessions. To unlock a user-locked session, the user must provide the correct identity with a valid authenticator.
O.WARNING_BANNER	All authorized users are notified that they are subject to being monitored, recorded, and audited through the use of an NNSA approved warning text and positive acknowledgement by the user is required before granting the user access to system resources.

This page intentionally blank.

ATTACHMENT 3

FUNCTIONALITY PROTECTION OBJECTIVES BY INFORMATION GROUP

The functionality protection objectives in the following table integrate the NNSA Cyber Security Threat Assessment and NNSA cyber security policies and are the minimum objectives for each information group that must be addressed in protection profiles for the information group.

Table 3. Protection Objectives by Information Group

	Open Unrestricted Access	Unclassified Protected	Unclassified Mandatory Protection	Confidential Non-Weapons Data	Secret Non-Weapons-Data	CRD Sigma 1 - 13	SRD Sigma 1 - 13	SRD Sigma 14 & 15	Top Secret	Top Secret Restricted Data
O.ACCESS	X	X	X	X	X	X	X	X	X	X
O.ACCESS_AUTH_L				X		X				
O.ACCESS_AUTH_Q					X		X	X	X	X
O.ACCESS_FORMAL	X	X	X	X	X	X	X	X	X	X
O.ACCESS_HISTORY	X	X	X	X	X	X	X	X	X	X
O.ACCESS_MALICIOUS	X	X	X	X	X	X	X	X	X	X
O.ALT_POWER_SUPPLY										
O.AUDIT_AUTOMATED_REVIEW						X	X	X	X	X
O.AUDIT_BASIC	X	X	X	X	X	X	X	X	X	X
O.AUDIT_CONTINOUS_MONITORING								X	X	X
O.AUDIT_FAILURE			X	X	X	X	X	X	X	X
O.AUDIT_PROTECTION	X	X	X	X	X	X	X	X	X	X
O.AUDIT_REVIEW	X	X	X	X	X	X	X	X	X	X
O.AUDIT_SELECTED_EVENTS				X	X	X	X	X	X	X
O.AUTHENT_EXPOSE	X	X	X	X	X	X	X	X	X	X
O.AUTHORIZATION	X	X	X	X	X	X	X	X	X	X
O.AUTHORIZE_NON_TOE:	X	X	X	X	X	X	X	X	X	X
O.AVAILABILITY_HIGH										
O.AVAILABILITY_LOW			X	X	X	X	X	X		
O.AVAILABILITY_MEDIUM										
O.BACKUP_ESSENTIAL										
O.CLEARING	X	X	X	X	X	X	X	X	X	X
O.COVERT_CHANNEL_REMOVE									X	X
O.COVERT_CHANNEL_REVIEW								X	X	X
O.CREDENTIAL_PROTECTION	X	X	X	X	X	X	X	X	X	X
O.CTL_IF_FAILSECUR										

	Open Unrestricted Access	Unclassified Protected	Unclassified Mandatory Protection	Confidential Non-Weapons Data	Secret Non-Weapons-Data	CRD Sigma 1 - 13	SRD Sigma 1 - 13	SRD Sigma 14 & 15	Top Secret	Top Secret Restricted Data
O.CTL_IF_PLATFORM										
O.CTL_IF_ROUTING										
O.CTL_IF_USR_CODE										
O.CTL_IF_FAILSECURE										
O.CTL_IF_POLICIES										
O.DATA_BACKUP_BASIC		X	X	X	X	X	X	X	X	X
O.DATA_BACKUP_EXTENDED									X	X
O.DATA_CHANGES_DETECTED	X	X								
O.DATA_CHANGES_DETERRED			X	X	X	X	X	X		
O.DATA_CHANGES_PREVENTED									X	X
O.DETECT_EXTERNAL_BASIC	X	X	X	X	X	X	X	X	X	X
O.DETECT_EXTERNAL_SOPHISTICATED				X	X	X	X	X	X	X
O.DETECT_HOST_BASIC	X	X	X	X	X	X	X	X	X	X
O.DETECT_HOST_SOPHISTICATED				X	X	X	X	X	X	X
O.DETECT_NETWORK_BASIC	X	X	X	X	X	X	X	X	X	X
O.DETECT_NETWORK_SOPHISTICATED				X	X	X	X	X	X	X
O.DETECT_SITE_BASIC	X	X	X	X	X	X	X	X	X	X
O.DETECT_SITE_SOPHISTICATED				X	X	X	X	X	X	X
O.ENTRY_NON_TECHNICAL	X	X	X	X	X	X	X	X	X	X
O.ENTRY_NON_TOE	X	X	X	X	X	X	X	X	X	X
O.ENTRY_TOE	X	X	X	X	X	X	X	X	X	X
O.FAIL_SECURE										
O.FORENSICS_PROC	X	X	X	X	X	X	X	X	X	X
O.FULL_RESIDUAL_PROTECTION				X	X	X	X	X	X	X
O.HARDWARE_EXAM_BASIC					X	X	X			
O.HARDWARE_EXAM_COMPREHENSIVE								X	X	X
O.HARDWARE_EXAM_MINIMUM	X	X	X	X						
O.ID_DISABLE	X	X	X	X	X	X	X	X	X	X
O.ID_REMOVAL	X	X	X	X	X	X	X	X	X	X
O.ID_REVALIDATION	X	X	X	X	X	X	X	X	X	X
O.INFO_FLOW	X	X	X	X	X	X	X	X	X	X
O.INTEGRITY_HIGH										
O.INTEGRITY_LOW	X	X	X	X	X	X	X	X		
O.INTEGRITY_MEDIUM										
O.INTEGRITY_VERY_HIGH									X	X
O.MALICIOUS_CODE	X	X	X	X	X	X	X	X	X	X

	Open Unrestricted Access	Unclassified Protected	Unclassified Mandatory Protection	Confidential Non-Weapons Data	Secret Non-Weapons-Data	CRD Sigma 1 - 13	SRD Sigma 1 - 13	SRD Sigma 14 & 15	Top Secret	Top Secret Restricted Data
O.MANAGE_TOE	X	X	X	X	X	X	X	X	X	X
O.MARK_COMPONENT		X	X	X	X	X	X	X	X	X
O.MARK_OUTPUT		X	X	X	X	X	X	X	X	X
O.MEDIA_REVIEW		X	X	X	X	X	X	X	X	X
O.NETWORK_INTERFACE	X	X	X	X	X	X	X	X	X	X
O.NTK_NNSA	X	X	X	X	X	X	X	X	X	X
O.ORIGIN_PROOF								X	X	X
O.PHY_CLASSIFIED				X	X	X	X	X	X	X
O.PHY_PROT_UNCLASSIFIED		X								
O.PHYS_MANDATED			X							
O.PHYSICAL	X	X	X	X	X	X	X	X	X	X
O.PHYSICAL_PROTECTION	X	X	X	X	X	X	X	X	X	X
O.RECEIPT_PROOF								X	X	X
O.RECOVERY_CONTROLLED	X	X	X	X	X					
O.RECOVERY_SECURE						X	X	X	X	X
O.REPLAY								X	X	X
O.RESIDUAL_PROTECTION	X	X	X	X	X	X	X	X	X	X
O.RESOURCE_USAGE			X	X	X	X	X	X	X	X
O.ROLE_SYS_ADM_&_ISSO				X	X	X	X	X	X	X
O.ROLES_OTHER_SECURITY			X	X	X	X	X	X	X	X
O.ROLES_TWO_PERSON								X	X	X
O.SANITIZATION				X	X	X	X	X	X	X
O.SEC_FUNC_MANAGEMENT	X	X	X	X	X	X	X	X	X	X
O.SECURITY_LEVEL_CHANGES								X	X	X
O.SESSION_ESTABLISHMENT	X	X	X	X	X	X	X	X	X	X
O.SOFTWARE_EXAM_BASIC					X	X	X			
O.SOFTWARE_EXAM_COMPREHENSIVE								X	X	X
O.SOFTWARE_EXAM_MINIMUM	X	X	X	X						
O.SUBJECT_DOMAIN_SEPARATION						X	X	X	X	X
O.TRAINING	X	X	X	X	X	X	X	X	X	X
O.TRANS_SEC_CLASS				X	X	X	X	X	X	X
O.TRANS_SEC_UNCLASS		X	X							
O.TRUSTED_PATH	X	X	X	X	X	X	X	X		
O.TRUSTED_PATH_COMMO									X	X
O.TSF_DOMAIN_SEPARATION	X	X	X	X	X	X	X	X	X	X
O.UNESCORT_ACCESS_CLASSIFIED				X	X	X	X	X	X	X

	Open Unrestricted Access	Unclassified Protected	Unclassified Mandatory Protection	Confidential Non-Weapons Data	Secret Non-Weapons-Data	CRD Sigma 1 - 13	SRD Sigma 1 - 13	SRD Sigma 14 & 15	Top Secret	Top Secret Restricted Data
O.UNESCORT_ACCESS_UNCLASS	X	X	X							
O.USER_INACTIVITY		X	X	X	X	X	X	X	X	X
O.USER_LOCKING	X		X	X	X	X	X	X	X	X
O.WARNING_BANNER	X	X	X	X	X	X	X	X	X	X

ATTACHMENT 4

ASSURANCE COMPONENTS BY ASSURANCE LEVEL

		Consequence of Loss				
		VL	L	M	H	VH
Evaluation Assurance Level (AL)	**Assurance Component**					
AL 1 - Functional	ACM_CAP.1 Version numbers		X			
	ADO_IGS.1 Installation, generation, and start-up procedures		X			
	ADV_FSP.1 Informal functional specification		X			
	ADV_RCR.1 Informal correspondence demonstration		X			
	AGD_ADM.1 Administrator guidance		X			
	AGD_USR.1 User guidance		X			
	ALC_FLR.1 Basic flaw remediation		X			
	ATE_IND.1 Independent testing - conformance		X			
AL 2 - Structurally Tested	ACM_CAP.2 Configuration items			X		
	ADO_DEL.1 Delivery procedures			X		
	ADO_IGS.1 Installation, generation, and start-up procedures			X		
	ADV_FSP.1 Informal functional specification			X		
	ADV_HLD.1 Descriptive high-level design			X		
	ADV_RCR.1 Informal correspondence demonstration			X		
	AGD_ADM.1 Administrator guidance			X		
	AGD_USR.1 User guidance			X		
	ALC_FLR.1 Basic flaw remediation			X		
	ATE_COV.1 Evidence of coverage			X		
	ATE_FUN.1 Functional testing			X		
	ATE_IND.2 Independent testing - sample			X		
	AVA_SOF.1 Strength of TOE security function evaluation			X		
	AVA_VLA.1 Developer vulnerability analysis			X		
AL 3 - Methodically Tested And Checked	ACM_CAP.3 Authorization controls				X	
	ACM_SCP.1 TOE CM coverage				X	
	ADO_DEL.1 Delivery procedures				X	
	ADO_IGS.1 Installation, generation, and start-up procedures				X	
	ADV_FSP.1 Informal functional specification				X	
	ADV_HLD.2 Security enforcing high-level design				X	
	ADV_RCR.1 Informal correspondence demonstration				X	
	AGD_ADM.1 Administrator guidance				X	

		Consequence of Loss				
		VL	L	M	H	VH
	AGD_USR.1 User guidance				X	
	ALC_DVS.1 Identification of security measures				X	
	ALC_FLR.2 Flaw reporting procedures				X	
	ATE_COV.2 Analysis of coverage				X	
	ATE_DPT.1 Testing: high-level design				X	
	ATE_FUN.1 Functional testing				X	
	ATE_IND.2 Independent testing - sample				X	
	AVA_MSU.1 Examination of guidance				X	
	AVA_SOF.1 Strength of TOE security function evaluation				X	
	AVA_VLA.1 Developer vulnerability analysis				X	
AL 4 - Methodically Designed, Tested, And Reviewed	ACM_AUT.1 Partial CM automation					X
	ACM_CAP.4 Generation support and acceptance procedures					X
	ACM_SCP.2 Problem tracking CM coverage					X
	ADO_DEL.1 Detection of modification					X
	ADO_IGS.1 Installation, generation, and start-up procedures					X
	ADV_FSP.1 Fully defined external interfaces					X
	ADV_HLD.2 Security enforcing high-level design					X
	ADV_IMP.1 Subset of the implementation of the TSF					X
	ADV_RCR.1 Informal correspondence demonstration					X
	ADV_SPM.1 Informal TOE security policy model					X
	AGD_ADM.1 Administrator guidance					X
	AGD_USR.1 User guidance					X
	ALC_DVS.1 Identification of security measures					X
	ALC_FLR.3 Systematic flaw remediation					X
	ALC_LCD.1 Developer defined life-cycle model					X
	ATE_COV.2 Analysis of coverage					X
	ATE_DPT.1 Testing: high-level design					X
	ATE_FUN.1 Functional testing					X
	ATE_IND.2 Independent testing - sample					X
	AVA_MSU.2 Validation of analysis					X
	AVA_SOF.1 Strength of TOE security function evaluation					X
	AVA_VLA.2 Independent vulnerability analysis					X