US GOVERNMENT PROTECTION PROFILE

USDA INSTRUMENT GRADING SYSTEMS FOR BASIC ROBUSTNESS ENVIRONMENTS

United States Department of Agriculture

16 September 2008
Version 1.0

Forward

This publication, "*US Government Protection Profile for USDA Instrument Grading Systems for Basic Robustness Environments"* is issued by the United States Department of Agriculture (USDA), Marketing and Regulatory Programs, Agricultural Marketing Service. This protection profile is based on the *Common Criteria for Information Technology Security Evaluations*, Version 3.1.

Further information can be found on the internet at: http://www.niap-ccevs.org/pp/.

Comments on this document should be directed to: ppcomments@niap-ccevs.org. The comments should include the title of the document, the page, the section number, and paragraph number, detailed comment and recommendations.

Table of Contents

List of Figures

List of Tables

{This page intentionally left blank}

1 Introduction

This Protection Profile (PP) is sponsored by the United States Department of Agriculture (USDA), Agricultural Marketing Service to provide secure implementations of Instrument Grading Systems, and is intended for the following uses:

1) For vendors and security evaluators, this PP defines the requirements that must be addressed by specific products as documented in vendor Security Targets (STs).

2) For vendors, system integrators and end users, this PP is useful in identifying areas that need to be addressed to provide secure system solutions.

The PP defines the requirements for a generic implementation of an Instrument Grading System that may be used in a processing plant overseen by USDA Graders. Relative to these requirements the PP includes:

1) Assumptions about the security aspects of the environment in which the TOE will be used;

2) Threats that are to be addressed by the TOE and its environment;

3) Security objectives of the TOE and its environment;

4) Functional and assurance requirements to meet those security objectives; and

5) Rationale demonstrating how the requirements meet the security objectives, and how the security objectives address the threats.

1.1 Identification

Title: U.S. Government Protection Profile for USDA Instrument Grading Systems for Basic Robustness Environments

Sponsor: United States Department of Agriculture, Agricultural Marketing Service

Developer: COACT Inc. and Common Criteria Consulting LLC

CC Version: Common Criteria (CC) Version 3.1, and applicable international and NIAP interpretations as of 28 January 2008.

Protection Profile Version: Version 1.0, dated 16 September 2008.

Evaluation Assurance Level: Basic Robustness Assurance consisting of all of the assurance requirements included in Evaluated Assurance Level (EAL) 2 (ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2, AVA_VAN.2) augmented with ALC_FLR.2 (Flaw reporting procedures).

Keywords: Basic Robustness Environments, Instrument Grading Systems.

1.2 Protection Profile Overview

This PP specifies the minimum security requirements for Instrument Grading Systems (i.e., the Target of Evaluation (TOE)) used in processing plants overseen by USDA Graders in Basic Robustness Environments. Instrument Grading Systems provide automated grading of products (e.g., beef) as well as records of the grading process, and are considered to provide sufficient

assurance for the grading process for environments where the likelihood of an attempted compromise is low.

1.2.1 Usage and Major Security Features of the TOE

The USDA supplies Graders to processing plants to grade carcasses according to standards developed by the USDA. Grading is based upon factors such as weight, marbling, maturity and lean firmness of the carcass. Grading has historically been done manually by the Graders, typically inspecting the carcasses in real time as they pass a grading station. A process chart illustrating the historical process is provided in Figure 1.1.

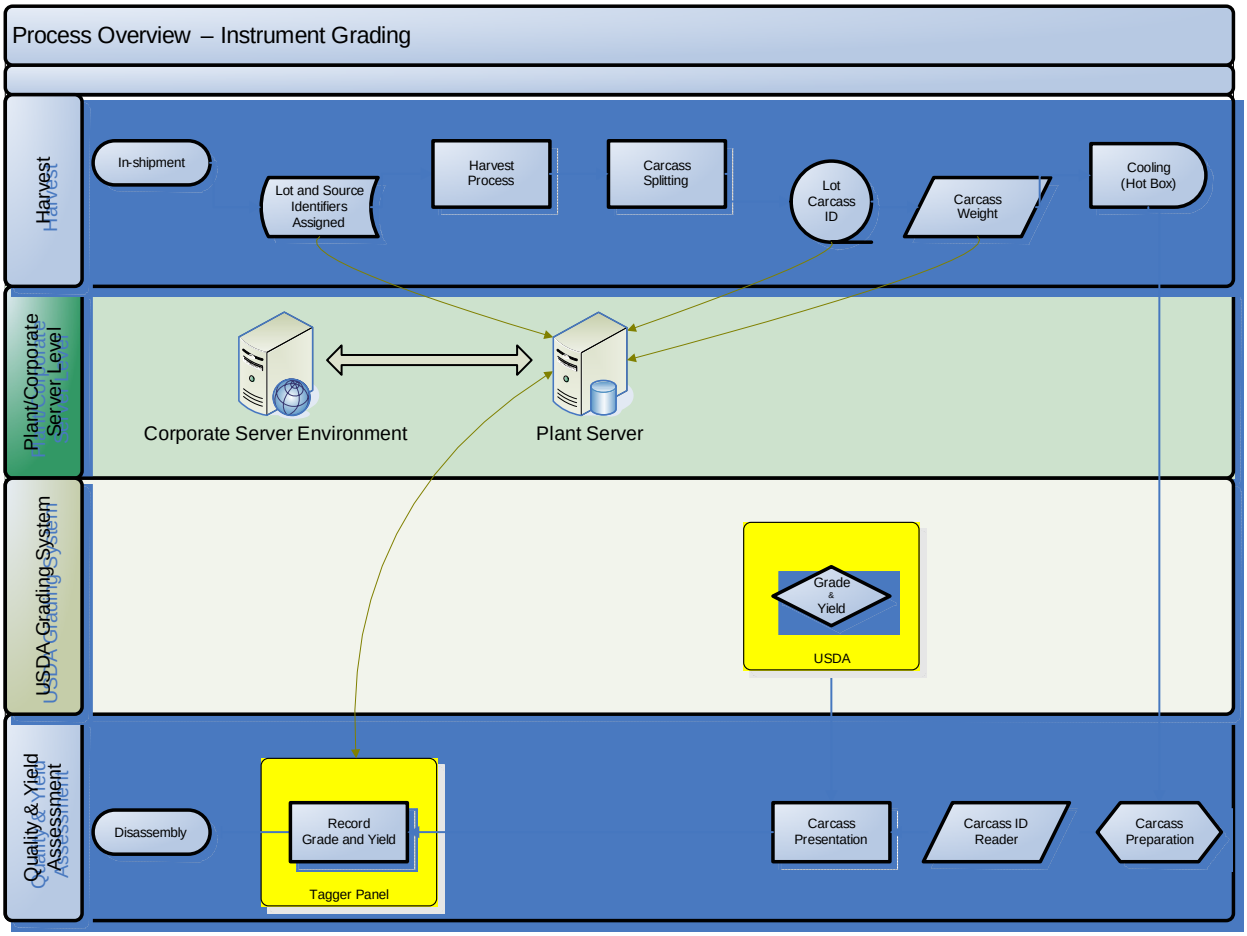

Figure 1.1 - Historical USDA Grading Process

Focusing on the grading in this process, a USDA Grader inspects and grades the carcass (as shown in the USDA Grading System row) based upon the Carcass Presentation step in the Quality and Yield Assessment row. The grade is assigned to the carcass by stamping it with a label, which is then recorded at the Tagger Panel for storage in the Plant Server (and potentially in the Corporate Server Environment). The assigned grade, along with other parameters concerning each carcass, is used by the processing plant to monitor and evaluate the processing operation.

The USDA desires to reduce the variation of the grading process, both within and between processing plants, as well as increase the precision, accuracy and resolution of the grades assigned to the carcasses. To this end, USDA has approved a prediction equation to be used in the processing plants for accurately and precisely predicting intramuscular marbling. When combined with carcass imaging capability in an IT system, the prediction equation can be used to automate the grading process to satisfy the USDA goals. Figure 1.2 illustrates the process utilizing this approach.

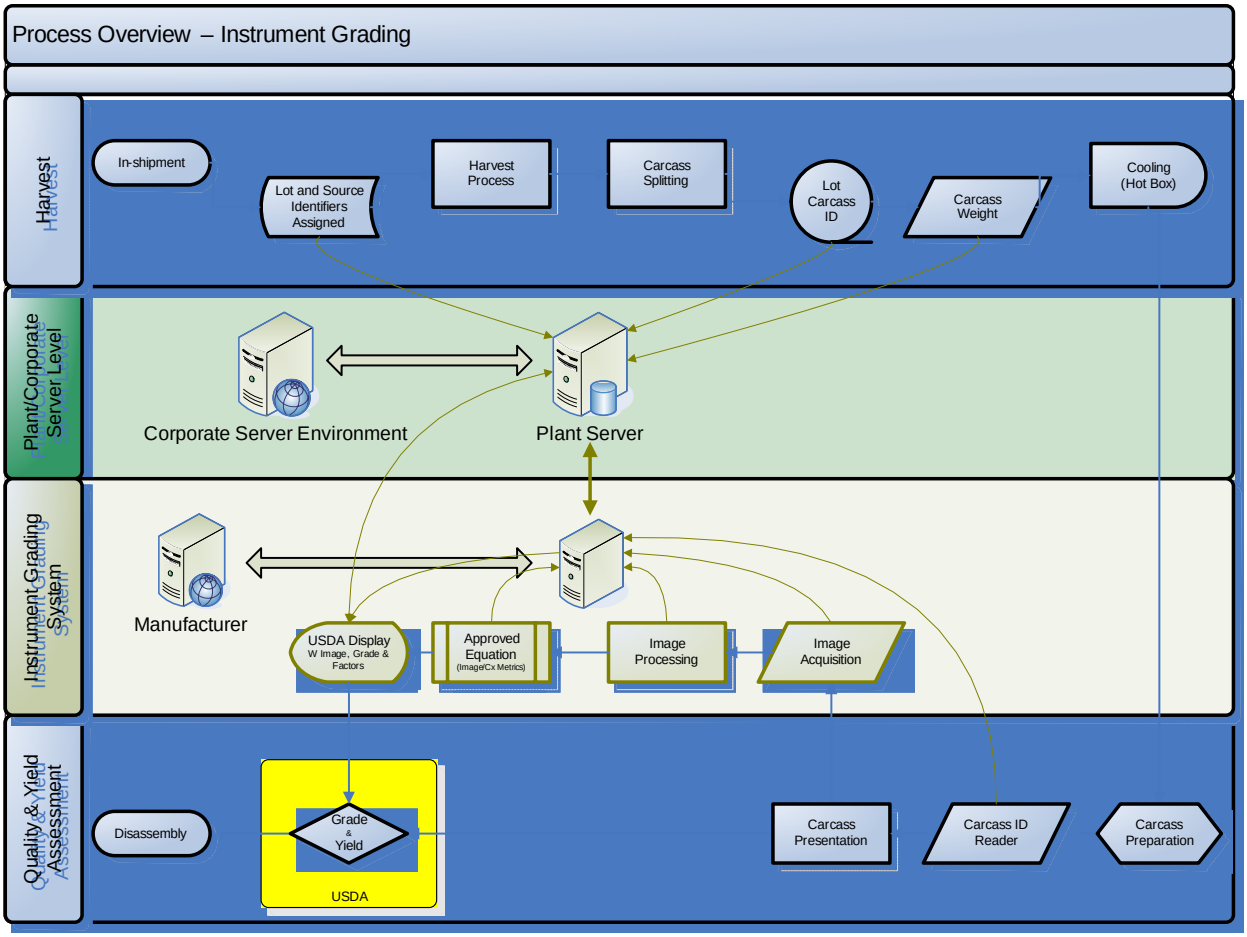

Figure 1.2 – USDA Grading Process Using Prediction Equation

The Instrument Grading System (IGS) interacts with other elements of the process as follows:

1) Parameters for each carcass (e.g., weight, lot, carcass identifier) are obtained from the Plant Server. Typical implementations of this information exchange use dedicated serial connections with specialized communication protocols or TCP/IP connections running over a LAN.

2) The Carcass ID for the carcass being inspected is obtained by scanning tags placed upon the carcass, via manual entry by plant personnel, or by association with the order of the carcass parameters supplied by the Plant Server. The IGS

may also support a combination of these techniques, such as reading a tag to suggest the carcass ID but allowing the value to be manually overridden.

3) One or more representative images (e.g., rib eye section for beef carcasses) of the carcass being inspected is captured by camera operators (hereafter referred to as Operators) and imported by the IGS. The captured image (typically of relatively high resolution such as TIFF) is analyzed and may be displayed to the Operators for them to assess the quality of (and possibly redo) the image. If the carcasses are processed in halves, both halves of the carcass may be imaged and evaluated by the TOE according to rules specified by the USDA.

4) The processed image (typically lower resolution such as JPEG) and calculated grade for the carcass (as well as other information) are displayed to the Grader. The Grader may override the calculated grade based upon the Grader's inspection of the carcass. The grade assigned to each carcass (either the calculated grade or the grade assigned by the Grader) is recorded by the TOE.

5) Information about each carcass is made available to the Plant Server. This information includes the carcass ID, calculated grade, and final grade (in case the calculated grade was overridden by the Grader); additional information such as the Operator ID and Grader ID is often provided. Typical implementations of this information exchange use dedicated serial connections with specialized communication protocols or TCP/IP connections running over a LAN.

6) The information used to calculate the grade for each carcass is classified as official memoranda under 7CFR54.2(b) and must be maintained on the IGS until delivered to the Grader. Typically this step is performed periodically via a portable storage device (e.g., flash drive) under the control of a Grader.

7) Plant personnel may be provided access to the captured images stored on the IGS for use in their monitoring and evaluation activities (in conjunction with the carcass information provided to the Plant Server). This access is restricted to the ability to review (but not modify or delete) the images and is provided via a TCP/IP connection running over a LAN.

8) The manufacturer of the TOE typically has remote access to the IGS for administrative tasks in support of the operational usage. This access is limited and is typically provided via a TCP/IP connection running over a LAN, with additional restrictions (e.g., VPN) imposed within the plant or corporate intranet.

Figure 1.2 shows the IGS as a single IT System (on which the TOE executes). This presentation is a logical representation of the IGS. In fact, it may be implemented on multiple interconnected systems based upon the following factors:

1) The number of cameras used to capture images of the carcasses. Each camera may be connected to a separate system.

2) Processing or storage requirements for the system. A single system may not have adequate resources to perform all of the TOE functions.

3) The architecture of the TOE. The TOE may be designed to operate on distributed systems.

If more than one system is used for the IGS, communication between the distributed components must be protected from modification.

The following figure presents a representative implementation of the TOE, with each function presented as a separate block. The TOE components are shaded while IT Environment components are not. Some blocks may have one or more instantiations (e.g., the number of "Camera Control" blocks is equal to the number of cameras present in each system). The blocks may execute on a single IT system or be distributed across multiple systems.

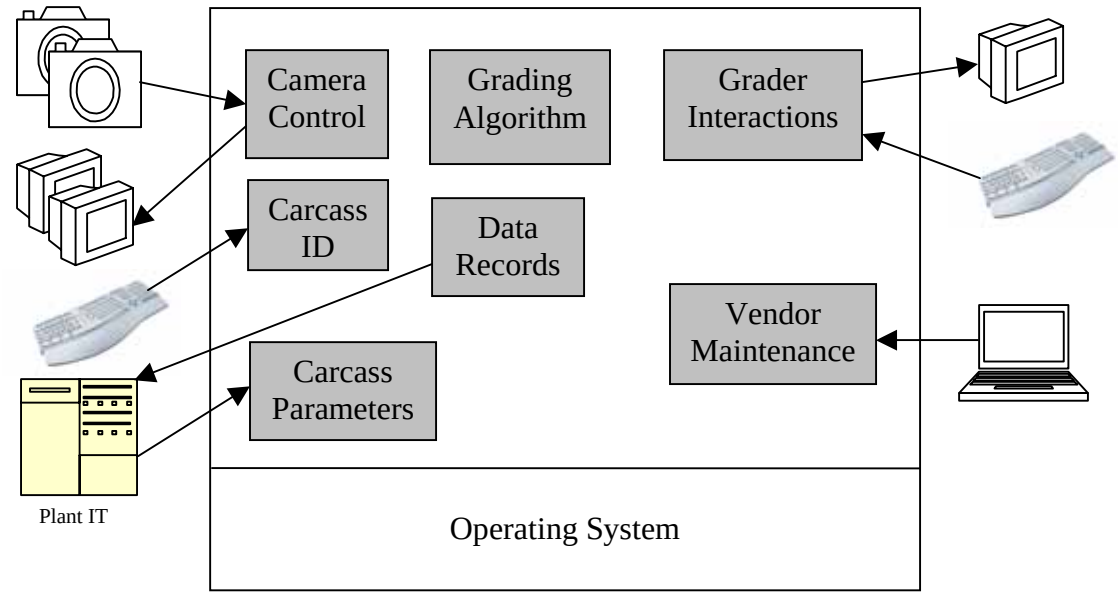

Figure 1.3 – Representative TOE Implementation

The TOE provides the following security features:

1) Access control – access to the captured and processed images (and other parameters used to calculate carcass grades) and other TSF data (e.g., identification and authentication credentials) is controlled based upon the role of the user.

2) Identification and authentication (I&A) – all users of the TOE must identify and authenticate themselves before being granted access.

3) Management – a defined set of management functions is provided for use by specific roles to manage the TOE.

4) Audit – all changes to controlled data made via the management interfaces, as well as other specified actions, must be audited. Audit logs must be able to be reviewed by specified roles.

5) Self test – upon start-up, the TOE performs specified self tests to ensure the integrity of the TOE.

In order to provide the functionality described in this PP, the following roles are assumed:

1) Operators operate the cameras to capture carcass images. They create the images used in the calculations and are allowed to view the image just captured to determine if it should be redone. They may also have the ability to input or change the carcass ID of the carcass being imaged. Operators interact with the TOE via the cameras and input/output device associated with Carcass Presentation. Operators must identify and authenticate themselves to the TOE.

2) Graders are USDA personnel that have final authority to determine the carcass grade and stamp the carcass. They can view information used by the TOE to calculate the grade and can override the calculated grade (the changed grade must be input to the TOE for tracking purposes). The Graders may initiate the transfer of the saved images and data records to a portable storage device to satisfy the requirements for official memoranda under 7CFR54.2(b). Graders must identify and authenticate themselves to the TOE before gaining access to any controlled functions. Graders interact with the TOE via the input/output device for the Grade & Yield step. The ability to transfer saved data may be provided via this same device or by a separate device.

3) Technicians are plant personnel responsible for IGS maintenance tasks such as changing cameras, calibrating cameras, and configuring communication parameters for TOE connections to other components and systems. This role also maintains the Operator access credentials. Technicians interact with the TOE via a locally attached terminal or remotely via the TCP/IP network. Technicians must identify and authenticate themselves to the TOE before gaining access to any controlled functions.

4) Vendors are personnel of the manufacturers that access the TOE to perform administrative functions in support of the operation of the TOE. Specific functions performed by Vendors are updating the TOE and updating the identification and authentication credentials for Graders. Vendors interact with the TOE via a locally attached terminal (typically only during initial installation) or remotely via the TCP/IP network. Vendors must identify and authenticate themselves to the TOE before gaining access to any controlled functions.

5) Reviewers are plant personnel that have been designated to have access to the IGS to view (read) stored images. Reviewers interact with the IGS remotely via the TCP/IP network. Reviewers must identify and authenticate themselves to the IT Environment before gaining access to the stored images. This role is only known in the IT Environment.

6) SysAdmins are plant personnel responsible for administrative functions on the IT systems hosting the TOE, but do not have any access to functions within the TOE. SysAdmins interact with the IT systems via a locally attached terminal or remotely via the TCP/IP network. SysAdmins must identify and authenticate

themselves to the IT Environment before gaining access to the IT systems. This role is only known in the IT Environment.

1.2.2 TOE Type

The product type of the Target of Evaluation (TOE) described in this Protection Profile (PP) is an application designed to implement the Instrument Grading System as defined by the USDA. The application is assumed to execute on top of an operating system and hardware that are part of the IT Environment.

1.2.3 Available non-TOE Hardware/Software/Firmware

The PP includes security requirements associated with a TOE as part of a larger system (i.e., running on a server on top of an operating system). As a component of these systems the TOE must work in concert with other components to provide system security services. While the PP includes requirements for component security functions to support system security services, it doesn't specify protocols or standards for compliance.

The TOE relies upon the IT Environment to perform the I&A function for some roles. The IT Environment also provides access control to the saved images for Reviewers. The TOE relies upon the IT Environment to limit network access to the IGS to those systems and personnel that have a specific need for access.

If the IGS is implemented as a distributed system, the IT Environment is relied upon to protect the integrity of communication between the distributed components.

1.3 Conventions

The following formatting conventions apply to the TOE Security Functional Requirements and the Requirements for the IT Environment.

The CC allows several operations to be performed on functional requirements; *refinement, selection, assignment,* and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this PP.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value underlined, assignment value.

Application notes provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text*.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number). (*) refers to all iterations of a component.

This PP contains several assignment and selection operations left to the ST writer to perform. The notation convention used for these is identical to that used in the Common Criteria.

1.4 Glossary of terms

Access — Interaction between an entity and an object that results in the flow or modification of data.

Access Control — Security service that controls the use of resources[1] and the disclosure and modification of data.[2]

Access Control Decision Function — A specialized function that makes access control decisions by applying access control policy rules to an access request.

Accountability — Property that allows activities in an IT system to be traced to the entity responsible for the activity.

Administrator — A user who has been specifically granted the authority to manage the TOE or a subset of the TOE, and whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.

Application Note — Supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.

Assurance — A measure of confidence that the security features of an IT system are sufficient to enforce its' security policy.

Attack — An intentional act attempting to violate the security policy of an IT system.

Attribute — A property that is associated with an entry. Attributes may be of a user type or operational type. User attributes are those attributes accessible by users. Operational attributes are attributes used by the directory and not accessible by users. An attribute is made up of attribute values and attribute type. The attribute type defines how the attribute value is used and processed. Attributes may be mandatory or optional.

Audit — To conduct an internal or independent review and assessment of records and/or activities.

Authentication — Security measure that verifies a claimed identity.

Authentication Data — Information used to verify a claimed identity.

Authorization — Permission, granted by an entity authorized to do so, to perform functions and access data.

Authorized User — An authenticated user who may, in accordance with the TSP, perform an operation.

Captured Image – by camera operators and imported by the Instrument Grading System (IGS) for analysis and processing.

Carcass Parameter – The input parameters the Instrument Grading System utilizes for analyzing the captured carcass images. The parameters include carcass lot and identifiers, and carcass weight.

---

[1] Hardware and Software

[2] Stored or communicated.

Common Criteria — The Common Criteria represents the outcome of a series of efforts to develop criteria for evaluation of IT security that are broadly useful within the international community.

Compromise — Violation of a security policy.

Confidentiality — A security policy pertaining to disclosure of data.

Connectivity — The property of the TOE that allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

Correlate - Refers to the correlation of carcass identifiers with images, so that the TOE may combine data from each to calculate a grade and produce a corresponding data record.

Data Record – A record containing a reference to the captured and processed image, carcass parameters, and carcass grade.

Defense-in-Depth (DID) — A security design strategy whereby layers of protection are utilized to establish an adequate security posture for an IT system.

Dependency — A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.

Entity — A subject, object, user or another IT device, which interacts with TOE objects, data, or resources.

Evaluation Assurance Level (EAL) — A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

External IT entity — Any trusted Information Technology (IT) product or system, outside of the TOE, which may, in accordance with the TSP, perform an operation.

Human User — Any person who interacts with the TOE.

Identity — A representation (e.g. a string) uniquely identifying an authorized user, which can be either the full or abbreviated name of that user or a pseudonym.

Integrity — A security policy pertaining to the corruption of data and TSF mechanisms.

Object — An entity within the TSC that contains or receives information and upon which subjects perform operations. Examples include a RI entry, attribute, or object class.

Operating Environment — The total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.

Organizational Security Policies — One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

Package — A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.

Password — A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Platform — Typically a device that includes the hardware and software elements that support all or part of the functional requirements of the TOE applications.

Processed Image – A low-resolution image that is the product of the Instrument Grading System analyzing the captured carcass image and producing an image and carcass grade for display to the graders.

Product — A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

Protected Items — Data in the TOE that is protected using access control mechanisms.

Protection Profile (PP) — An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Refinement — The addition of details to a component.

Remote Trusted User — A trusted user or trusted external IT entity that accesses the TOE from a location outside the boundary of the TOE.

Robustness — A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly.

Role — A predefined set of rules establishing the allowed interactions between a user and the TOE.

Secret — Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.

Secure State — Condition in which all TOE security policies are enforced.

Security attribute — TSF data associated with subjects, objects, and users that are used for the enforcement of the TSP.

Security Policy — A precise specification of the security rules under which the TOE shall operate, including the rules derived from the requirements of this document and additional rules imposed by the vendor.

Security Target (ST) — A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Selection — The specification of one or more items from a list in a component.

Session – Whenever someone is logged in to the system.

Subject — An entity within the TSC that causes operations to be performed. Subjects can come in two forms: trusted and untrusted. Trusted subjects are exempt from part or all of the TOE security policies. Untrusted subjects are bound by all TOE security policies.

System — A specific IT installation, with a particular purpose and operational environment.

Target of Evaluation (TOE) — An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

Threat — Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.

Threat Agent — Any human user or Information Technology (IT) product or system, which may attempt to violate the TSP and perform an unauthorized operation with the TOE.

Time stamp — Electronic seal including a time and/or date indication applied over data.

TOE resource — Anything useable or consumable in the TOE.

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 Functions Interface (TSFI) — A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.

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

Trusted — Used to describe any user or IT entity that is authenticated to the TOE with some level of assurance.

Trusted channel — A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.

TSF data — Data created by and for the TOE that might affect the operation of the TOE.

TSF Scope of Control (TSC) — The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

User — Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User Data — Data created by and for the user that does not affect the operation of the TSF.

Vulnerability — A weakness that can be exploited to violate the TOE security policy.

1.5 Document Organization

Section 1 introduces this PP document through an overview, conventions, glossary of terms, and a description of this PP organization.

Section 2 provides a statement of Common Criteria Conformance.

Section 3 provides the security problem definition. This chapter states the threats, organizational security policies, and assumptions pertinent to the PP.

Section 4 identifies the security objectives satisfied by the TOE, the development environment of the TOE, and the operational environment of the TOE.

Section 5 provides the extended definition for any extended components not found in Part 2 or Part 3.

Section 6 specifies the security functional and assurance requirements for the TOE and its IT environment. It also provides the requirements rationale, which shows that the requirements meet the objectives and that all dependencies are satisfied.

1.6 References

[7CFR54.2] Code of Federal Regulations, Title 7, Volume 3, PART 54, Section 54.2, Revised as of January 1, 2002.

[BRCIM] Consistency Instruction Manual For Development of US Government Protection Profiles (PP) For use in Basic Robustness Environments, NIAP Protection Profile Review Board, Release 4.0.

[DM3530-001] USDA Departmental Manual DM3530-001, Amendment Number 1 to Departmental Manual, 07/20/05.

[DM3525-001] USDA Departmental Manual DM3525-001, USDA Internet Access Security for Private Internet Service Providers, 07/15/04.

[DM3535-001] USDA Departmental Manual DM3535-001, USDA's C2 Level of Trust, 02/17/05.

[DM3550-002] USDA Departmental Manual DM3550-002, Sensitive but Unclassified (SBU) Information Protection, 02/17/05.

[DM3555-000] USDA Departmental Manual DM3555-000, Certification and Accreditation of Information Systems, 10/18/05.

[DM3565-001] USDA Departmental Manual DM3565-001, Annual Security Plan Guide for IT Systems, 02/17/05.

[DR1110-002] USDA Departmental Regulation DR1110-002, Management Accountability and Control, 04/14/04.

[DR3140-001] USDA Departmental Regulation DR3140-001, USDA Information Systems Security Policy, May 15, 1996.

[DR3610-001] USDA Departmental Regulation DR3610-001, USDA eAuthentication Service, 11/04/04.

2 Conformance Claims

2.1 PP Conformance Claim

This Protection Profile is Common Criteria Part 2 Extended and Common Criteria Part 3 conformant, with U.S. DoD Basic Robustness Assurance (as defined in the *Consistency Instruction Manual For development of US Government Protection Profiles (PP) For use in Basic Robustness Environments* [BRCIM]).

Any ST claiming compliance to this PP must do so in a demonstrable manner. SFRs levied against the IT Environment in the PP (specified in section 6.2) may be implemented in the ST TOE.

STs claiming compliance may consist of software only.

2.2 PP conformance claim rationale

The EAL definitions and assurance requirements in Part 3 of the CC were reviewed and the *Basic Robustness Assurance Package* as defined in [BRCIM] was believed to best achieve the goal of addressing circumstances where developers and users require a low level of independently assured security in commercial products. The assurance package was selected because the TOE is an application executing on a system outside the TOE boundary, and basic is the highest robustness level available to application TOEs.

3 Security Problem Definition

This section discusses the characteristics of environments and threat levels appropriate for basic robustness TOEs, and it describes the specific security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed. This information is provided to help organizations using this PP insure that the functional requirements specified by this PP are appropriate for their intended application of a compliant TOE.

This section includes the following:

1) Discussion of basic robustness;
2) Assumptions about the security aspects of a compliant TOE environment;
3) Threats to TOE assets or to the TOE environment which must be countered; and
4) Organizational security policies that compliant TOEs must enforce.

3.1 Characterizing BASIC robustness

Robustness is defined as a TOE characteristic that describes how well the TOE can protect itself and its resources. The more robust the TOE, the better it is able to protect itself. This section relates the defining factors of the IT environment, authorization, and value of resources to the selection of appropriate robustness levels.

3.1.1 TOE Environment Defining Factors

In trying to specify the environments in which TOEs with various levels of robustness are appropriate, it is useful to first discuss the two defining factors that characterize that environment: value of the resources and authorization of the entities to those resources.

In general terms, the environment for a TOE can be characterized by the authorization (or lack of authorization) the least trustworthy entity has with respect to the highest value of TOE resources (i.e. the TOE itself and all of the data processed by the TOE).

Note that there are an infinite number of combinations of entity authorization and value of resources; this conceptually “makes sense” because there are an infinite number of potential environments, depending on how the resources are valued by the organization, and the variety of authorizations the organization defines for the associated entities. In the next section, these two environmental factors will be related to the robustness required for selection of an appropriate TOE.

Value of Resources

Value of the resources associated with the TOE includes the data being processed or used by the TOE, as well as the TOE itself (for example, a real-time control processor). “Value” is assigned by the using organization. For example, in the DoD low-value data might be equivalent to data marked “FOUO”, while high-value data may be those classified Top Secret. In a commercial enterprise, low-value data might be the internal organizational structure as captured in the corporate on-line phone book, while high-value data might be corporate research results for the next generation product. Note that when considering the value of the data one must also consider the value of data or resources that are accessible through exploitation of the TOE. For example, a firewall may have “low value” data itself, but it might protect an enclave with high value data. If

the firewall was being depended upon to protect the high value data, then it must be treated as a high-value-data TOE.

Authorization of Entities

Authorization that entities (users, administrators, other IT systems) have with respect to the TOE (and thus the resources of that TOE, including the TOE itself) is an abstract concept reflecting a combination of the trustworthiness of an entity and the access and privileges granted to that entity with respect to the resources of the TOE. For instance, entities that have total authorization to all data on the TOE are at one end of this spectrum; these entities may have privileges that allow them to read, write, and modify anything on the TOE, including all TSF data. Entities at the other end of the spectrum are those that are authorized to few or no TOE resources. For example, in the case of a router, non-administrative entities may have their packets routed by the TOE, but that is the extent of their authorization to the TOE's resources. In the case of an OS, an entity may not be allowed to log on to the TOE at all (that is, they are not valid users listed in the OS's user database).

It is important to note that authorization does not refer to the access that the entities actually have to the TOE or its data. For example, suppose the owner of the system determines that no one other than employees was authorized to certain data on a TOE, yet they connect the TOE to the Internet. There are millions of entities that are not authorized to the data (because they are not employees), but they actually have connectivity to the TOE through the Internet and thus can attempt to access the TOE and its associated resources.

Entities are characterized according to the value of resources to which they are authorized; the extent of their authorization is implicitly a measure of how trustworthy the entity is with respect to compromise of the data (that is, compromise of any of the applicable security policies; e.g., confidentiality, integrity, availability). In other words, in this model the greater the extent of an entity's authorization, the more trustworthy (with respect to applicable policies) that entity is.

3.1.2 Selection of Appropriate Robustness Levels

As defined above, robustness describes how well the TOE can protect itself and its resources. The more robust the TOE, the better it is able to protect itself. This section relates the defining factors of the IT environment, authorization, and value of resources to the selection of appropriate robustness levels.

When assessing any environment with regards to Information Assurance (IA), the critical point to consider is the likelihood of a compromise. This likelihood is somewhat dependent on the value of the TOE and resident data as well as logical connectivity and physical location. It follows that as the likelihood of an attempted resource compromise increases, the robustness of an appropriate TOE should also increase. It is critical to note that several combinations of environmental factors will result in environments in which the likelihood of an attempted compromise is similar. Consider the following two cases:

1) The first case is a TOE that processes low-value data. This TOE is connected to the Internet and is accessible by authorized entities. In this case, the least trusted entities are unauthorized entities exposed to the TOE as a result of Internet connectivity. Since only low-value data is being processed, the likelihood that

unauthorized entities would attempt to gain access to the system is low. In this instance, TOE compliance with a basic robustness PP is sufficient.

2) The second case is a TOE that processes high-value information. In this example, the TOE is a stand-alone system that is both logically isolated from any external connections and is physically protected. Additionally, every entity with physical and logical access to the TOE holds the highest authorizations thereby assuring that only highly trusted users are authorized to access the TOE. In this case, even though high value information is processed, it is unlikely that a compromise of the TOE and resident information will occur simply because of the physical and logical isolation and the trustworthiness of the entities. Once again, selection of a basic robustness TOE is appropriate.

The preceding examples demonstrated that it is possible for different combinations of entity authorization/resource values to result in a similar likelihood of an attempted compromise. As mentioned earlier, the robustness of a system is an indication of the protection being provided to counter compromise attempts. Therefore, a basic robustness system should be sufficient to counter compromise attempts where the likelihood of an attempted compromise is low. The following chart depicts the “universe” of environments characterized by the two factors discussed in the previous section: on one axis is the authorization defined for the least trustworthy entity, and on the other axis is the highest value of resources associated with the TOE.

As depicted in Figure 3.1, the robustness of the TOEs required in each environment steadily increases as one goes from the upper left of the chart to the lower right; this corresponds to the need to counter increasingly likely attack attempts by the least trustworthy entities in the environment. Note that the shading of the chart is intended to reflects the notion that different environments engender similar levels of “likelihood of attempted compromise”, signified by a similar color. Further, the delineations between such environments are not stark, but rather are finely grained and gradual.

While it would be possible to create many different "levels of robustness" at small intervals along the “Increasing Robustness Requirements” line to counter the increasing likelihood of attempted compromise due to those attacks, it would not be practical or particularly useful. Instead, in order to implement the robustness strategy where there are only three robustness levels (Basic, Medium, and High), the graph is divided into three sections, with each section corresponding to set of environments where the likelihood of attempted compromise is roughly similar. This is graphically depicted in Figure 3.2.

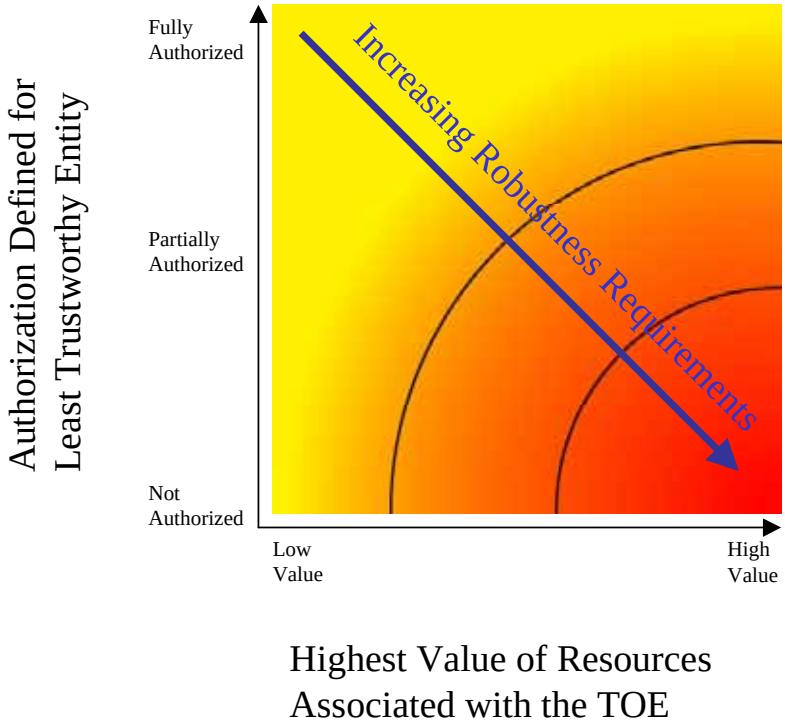

Figure 3.1 – Robustness Requirements

In Figure 3.2 the "dots" represent given instantiations of environments; like-colored dots define environments with a similar likelihood of attempted compromise. Correspondingly, a TOE with a given robustness should provide sufficient protection for environments characterized by like-colored dots. In choosing the appropriateness of a given robustness level TOE PP for an environment, then, the user must first consider the lowest authorization for an entity as well as the highest value of the resources in that environment. This should result in a "point" in the chart above, corresponding to the likelihood that that entity will attempt to compromise the most valuable resource in the environment. The appropriate robustness level for the specified TOE to counter this likelihood can then be chosen.

The difficult part of this activity is differentiating the authorization of various entities, as well as determining the relative values of resources; (e.g., what constitutes "low value" data vs. "medium value" data). Because every organization will be different, a rigorous definition is not possible.

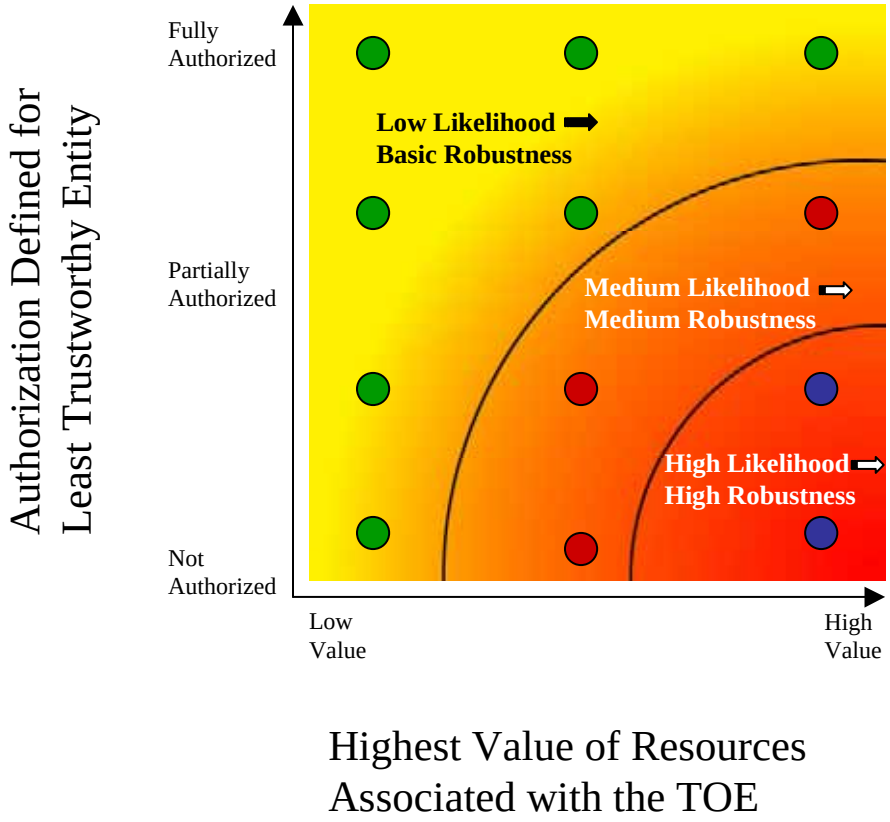

Figure 3.2 – Robustness Levels

3.1.3 Basic Robustness

Basic robustness TOEs falls in the upper left area of the previously discussed robustness figures. A Basic Robustness TOE is considered sufficient for low threat environments or where compromise of protected information will not have a significant impact on mission objectives. This implies that the motivation of the threat agents will be low in environments that are suitable for TOEs of this robustness. In general, basic robustness results in "good commercial practices" that counter threats based in casual and accidental disclosure or compromise of data protected by the TOE.

Threat agent motivation can be considered in a variety of ways. One possibility is that the value of the data process or protected by the TOE will generally be seen as of little value to the adversary (i.e., compromise will have little or no impact on mission objectives). Another possibility, (where higher value data is processed or protected by the TOE) is that procuring organizations will provide other controls or safeguards (i.e., controls that the TOE itself does not enforce) in the fielded system in order to increase the threat agent motivation level for compromise beyond a level of what is considered reasonable or expected to be applied.

3.2 Threats to Security

In addition to helping define the robustness appropriate for a given environment, the threat agent is a key component of the formal threat statements in the PP. Threat agents are typically characterized by a number of factors such as ***expertise***, ***available resources***, and ***motivation***.

Because each robustness level is associated with a variety of environments, there are corresponding varieties of specific threat agents (that is, the threat agents will have different combinations of motivation, expertise, and available resources) that are valid for a given level of robustness. The following discussion explores the impact of each of the threat agent factors on the ability of the TOE to protect itself (that is, the robustness required of the TOE).

The ***motivation*** of the threat agent seems to be the primary factor of the three characteristics of threat agents outlined above. Given the same expertise and set of resources, an attacker with low motivation may not be as likely to attempt to compromise the TOE. For example, an entity with no authorization to low value data none-the-less has low motivation to compromise the data; thus a basic robustness TOE should offer sufficient protection. Likewise, the fully authorized user with access to highly valued data similarly has low motivation to attempt to compromise the data, thus again a basic robustness TOE should be sufficient.

Unlike the motivation factor, however, the same can't be said for ***expertise***. A threat agent with low motivation and low expertise is just as unlikely to attempt to compromise a TOE as an attacker with low motivation and high expertise; this is because the attacker with high expertise does not have the motivation to compromise the TOE even though they may have the expertise to do so. The same argument can be made for ***resources*** as well.

Therefore, when assessing the robustness needed for a TOE, the motivation of threat agents should be considered a "high water mark". ***That is, the robustness of the TOE should increase as the motivation of the threat agents increases.***

Having said that, the relationship between expertise and resources is somewhat more complicated. In general, if resources include factors other than just raw processing power (money, for example), then expertise should be considered to be at the same "level" (low, medium, high, for example) as the resources because money can be used to purchase expertise. Expertise in some ways is different, because expertise in and of itself does not automatically procure resources. However, it may be plausible that someone with high expertise can procure the requisite amount of resources by virtue of that expertise (for example, hacking into a bank to obtain money in order to obtain other resources).

It may not make sense to distinguish between these two factors; in general, it appears that the only effect these may have is to lower the robustness requirements. For instance, suppose an organization determines that, because of the value of the resources processed by the TOE and the trustworthiness of the entities that can access the TOE, the motivation of those entities would be "medium". This normally indicates that a medium robustness TOE would be required because the likelihood that those entities would attempt to compromise the TOE to get at those resources is in the "medium" range. However, now suppose the organization determines that the entities (threat agents) that are the least trustworthy have no resources and are unsophisticated. In this case, even though those threat agents have medium motivation, the likelihood that they would be able to mount a successful attack on the TOE would be low, and so a basic robustness TOE may be sufficient to counter that threat.

It should be clear from this discussion that there is no "cookbook" or mathematical answer to the question of how to specify exactly the level of motivation, the amount of resources, and the degree of expertise for a threat agent so that the robustness level of TOEs facing those threat agents can be rigorously determined. However, an organization can look at combinations of

these factors and obtain a good understanding of the likelihood of a successful attack being attempted against the TOE. Each organization wishing to procure a TOE must look at the threat factors applicable to their environment; discuss the issues raised in the previous paragraph; consult with appropriate accreditation authorities for input; and document their decision regarding likely threat agents in their environment. The important general points we can make are:

1) The motivation for the threat agent defines the upper bound with respect to the level of robustness required for the TOE.

2) A threat agent's expertise and/or resources that are "lower" than the threat agent's motivation (e.g., a threat agent with high motivation but little expertise and few resources) may lessen the robustness requirements for the TOE (see next point, however).

3) The availability of attacks associated with high expertise and/or high availability of resources (for example, via the Internet or "hacker chat rooms") introduces a problem when trying to define the expertise of, or resources available to, a threat agent.

Table 3.1 lists the threats to security.

Table 3.1 – Threats to Security

Threat	Description of Threat
T.AUDIT_ COMPROMISE	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.
T.CORRUPT_GRADING	Malicious users may corrupt the grading algorithm in the TOE to gain financial advantage.
T.CORRUPTED_ IMPLEMENTATION	Unintentional or intentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a malicious user or program.
T.FLAWED_DESIGN	Unintentional or intentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a malicious user or program.
T.MALICIOUS_TSF_ COMPROMISE	A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.RESOURCE_ EXHAUSTION	A malicious process or user may block others from system resources (e.g., disk space) via a resource exhaustion denial of service attack.
T.UNATTENDED_ SESSION	A user may gain unauthorized access to an unattended session.

Threat	Description of Threat
T.UNAUTHORIZED_ACCESS	A user may gain access to user data for which they are not authorized according to the TOE security policy.
T.UNIDENTIFIED_ACTIONS	The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.

3.3 Organizational Security Policies

Table 3.2 lists the organizational security policies.

Table 3.2 – Organizational Security Policies

Policy	Policy Description	Formal Reference
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which administrators consent by accessing the system.	USDA DR3140-001, Section 15
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.	USDA DM3550-002 USDA DM3555-000 USDA DM3565-001 USDA DR1110-002, Section 6, b
P.ADMIN_ACCESS	Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.	USDA DM3525-001
P.DATA_DELIVERY	The TOE shall maintain the captured and processed images used in calculating the grades and data records reflecting the grades until delivered to a USDA Grader.	7CFR54.2 (b)
P.I_AND_A	All users must be identified and authenticated prior to accessing any controlled resources with the exception of public objects.	USDA DR3610-001
P.ROLES	The TOE shall provide authorized administrator roles for secure administration of the TOE. These roles shall be separate and distinct from other authorized users.	USDA DM3535-001, Section 4, d

Policy	Policy Description	Formal Reference
P.SYSTEM_INTEGRITY	The TOE shall provide the ability to periodically validate its correct operation.	USDA DM3555-000
P.VULNERABILITY_ ANALYSIS_TEST	The TOE must undergo appropriate independent vulnerability analysis and penetration testing to demonstrate that the TOE is resistant to an attacker possessing a basic attack potential.	USDA DM3530-001

3.4 Secure USAGE Assumptions

Table 3.3 lists the Secure Usage Assumptions.

Table 3.3 – Secure Usage Assumptions

Assumption	Description of Assumption
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NETWORK_ACCESS	Administrators will limit network access to the TOE and TOE data to authorized users with valid requirements for network access to the TOE.
A.NO_GENERAL_PURPOSE	The administrator ensures there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the systems on which the TOE executes.
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
A.ROBUST_ENVIRONMENT	It is assumed that the IT environment is at least as robust as the TOE.
A.SECURE_COMMS	It is assumed that the IT environment will provide secure communications between remote users and the IGS, and between distributed components of the TOE.
A.TRAINED_ ADMINISTRATORS	Authorized administrators (users with the Technician, Vendor or SysAdmin role) are appropriately trained and follow all administrator guidance
A.TRUSTED_INDIVIDUAL	If an individual is allowed to perform procedures upon which the security of the TOE may depend, it is assumed that the individual is trusted with assurance commensurate with the value of the IT assets.

4 Security Objectives

This chapter describes the security objectives. These security objectives are divided between the Security Objectives for the TOE, the Security Objectives for the Development Environment, and the Security Objectives for the Operating Environment.

4.1 Security Objectives for the TOE

Table 4.1 contains the Security Objectives for the TOE.

Table 4.1 – Security Objectives for the TOE

Objective	Description of Objective
O.ACCESS_GRADERS	The TOE will provide Graders the ability to perform the following: 1. identify and authenticate themselves 2. view captured and processed images and data records 3. override calculated grade assignments 4. transfer stored images and data records
O.ACCESS_OPERATORS	The TOE will provide Operators the ability to perform the following: 1. identify and authenticate themselves 2. capture and recapture images 3. view captured images as they are created 4. provide carcass identifiers 5. view data records
O.ACCESS_PLANTIT	The TOE will receive carcass parameters from the Plant IT systems and transmit data records to the Plant IT systems.
O.ACCESS_TECHNICIANS	The TOE will provide Technicians the ability to perform the following: 1. identify and authenticate themselves 2. configure Operator and Technician authentication credentials 3. change cameras 4. adjust camera parameters 5. configure communication with other systems 6. configure the security banner to be displayed to TOE users 7. view captured images, carcass parameters and data records 8. delete captured images and data records after they have been transferred to a Grader 9. delete carcass parameters after they are no longer required
O.ACCESS_VENDORS	The TOE will provide Vendors the ability to perform the following: 1. identify and authenticate themselves 2. configure Grader and Grader authentication credentials

Objective	Description of Objective
	3. update the TOE executable code 4. configure inactivity timers for roles within the TOE 5. view captured images, carcass parameters and data records 6. delete captured images and data records after they have been transferred to a Grader 7. delete carcass parameters after they are no longer required
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events associated with users.
O.DATA_DELIVERY	The TOE shall provide a mechanism to deliver soft copy of the captured and processed images used in calculating the grades and data records reflecting the grades to Graders.
O.DATA_PROTECTION	The TOE shall protect the captured and processed images used in calculating the grades and data records reflecting the grades from deletion or unauthorized modification (via mechanisms within the TSC) before the data has been delivered to Graders.
O.DATA_STORAGE	The TOE shall store captured and processed images used in calculating the grades and data records reflecting the grades for all grading operations.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.INACTIVITY	The TOE will terminate sessions that are inactive for longer than the configured timeout period.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.MEDIATE	The TOE must protect user data in accordance with its security policy.
O.SELFTEST	The TSF shall periodically perform self tests to verify it's own integrity.
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.

4.2 Security Objectives for the development Environment

Table 4.2 contains security objectives for the development environment.

Table 4.2 – Security Objectives for the Development Environment

Objective	Objective Description
OD.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure management.

Objective	Objective Description
OD.CONFIGURATION_IDENTIFICATION	The configuration of the TOE is fully identified in a manner that will allow known implementation errors to be correlated with operational systems.
OD.DELIVERY_INTEGRITY	The development environment shall ensure that the TOE is delivered to the consumer without compromising the integrity of the TOE.
OD.DEVELOPMENT_INTEGRITY	The development environment shall ensure that the integrity of the source code of the TOE is protected.
OD.DOCUMENTED_DESIGN	The design of the TOE is adequately and accurately documented.
OD.FLAW_REMEDIATION	Procedures to address security issues in the TOE will be documented and followed.
OD.PARTIAL_SELF_PROTECTION	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.
OD.TEST	The TOE will undergo testing by the developer and an independent party to detect obvious errors in the implementation.
OD.VULNERABILITY_ANALYSIS	The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.

4.3 Security Objectives for the operational Environment

Table 4.3 contains security objectives for the operational environment.

Table 4.3 – Security Objectives for the Operational Environment

Objective	Objective Description
OE.ACCESS_REVIEWERS	The IT Environment will provide Reviewers the ability to view stored images.
OE.ACCESS_SYSADMINS	The IT Environment will provide SysAdmins the ability to perform the following: 1. configure operating system access credentials 2. configure network access parameters 3. change the time setting 4. configure inactivity timers for roles outside the TOE 5. configure the security banner to be displayed to IT Environment users
OE.AUDIT_BACKUP	The IT administrator shall ensure that audit log files are backed up and can be restored, and that audit log files do not run out of disk space.
OE.AUDIT_GENERATION	The IT Environment will provide the capability to detect and create records of security-relevant events associated with users.

Objective	Objective Description
OE.AUDIT_REVIEW	The IT Environment will provide the capability to view audit information.
OE.AUDIT_STORAGE	The IT environment will provide a means for secure storage of the TOE audit log files.
OE.DATA_PROTECTION	The IT Environment shall protect the stored captured and processed images used in calculating the grades and data records reflecting the grades from deletion or modification (via mechanisms outside the TSC) before the data has been delivered to Graders.
OE.DEDICATED_ SYSTEMS	The IT administrator shall ensure that the IT systems on which the TOE executes are dedicated to that purpose and do not host general purpose computing facilities.
OE.DISPLAY_BANNER	The systems on which the TOE executes will display an advisory warning regarding use of the IT systems.
OE.I&A	The IT Environment shall identify all users and authenticate all users before allowing them access to the TOE or TOE data..
OE.INACTIVITY	The It Environment will terminate sessions that are inactive for longer than the configured timeout period.
OE.NETWORK_ACCESS	The IT administrator shall configure the network to which the TOE systems are attached such that connectivity between the TOE systems and other network assets is limited to the smallest required set of users and/or systems.
OE.NO_EVIL	Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.PHYSICAL_ACCESS	The operational environment of the TOE shall restrict physical access to the TOE to administrative personnel and maintenance personnel accompanied by administrative personnel.
OE.RESIDUAL_INFORMATION	The IT Environment will ensure that any information contained in a protected resource within the TOE's Scope of Control is not released when the resource is reallocated.
OE.SECURE_COMMS	The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.
OE.SELFTEST	The IT environment shall periodically perform self tests to verify the integrity of the abstract machine upon which the TOE depends.
OE.TIME_STAMPS	The IT environment will provide reliable time stamps.
OE.TOE_ACCESS	The IT Environment will provide mechanisms that control a user's logical access to the TOE.

Objective	Objective Description
OE.TRUST_IT	Each IT entity the TOE relies on for security functions will be installed, configured, managed and maintained in a manner appropriate to the IT entity, and consistent with the security policy of the TOE and the relationship between them.

4.4 Security Objectives Rational

4.4.1 Mapping of Threats to Objectives

The following table presents a mapping of the threats to the objectives defined in this PP. Only objectives that map to one or more of the threats is included in this table.

Table 4.4 – Mapping of Threats to Objectives

	T.AUDIT_ COMPROMISE	T.CORRUPT_GRADING	T.CORRUPTED_ IMPLEMENTATION	T.FLAWED_DESIGN	T.MALICIOUS_TSF_ COMPROMISE	T.MASQUERADE	T.RESIDUAL_DATA	T.RESOURCE_ EXHAUSTION	T.UNATTENDED_ SESSION	T.UNAUTHORIZED_ACCESS	T.UNIDENTIFIED_ ACTIONS
O.ACCESS_GRADERS								X			
O.ACCESS_OPERATORS								X			
O.ACCESS_PLANTIT								X			
O.AUDIT_GENERATION											X
O.INACTIVITY									X		
O.MEDIATE										X	
O.SELFTEST		X			X						
O.TOE_ACCESS		X			X	X		X			
OD.CONFIGURATION_ IDENTIFICATION			X	X							
OD.DELIVERY_INTEGRITY			X								
OD.DEVELOPMENT_ INTEGRITY			X								
OD.DOCUMENTED_DESIGN				X							
OD.FLAW_REMEDIATION			X	X							
OD.PARTIAL_SELF_PROTECTION		X			X						

	T.AUDIT_ COMPROMISE	T.CORRUPT_GRADING	T.CORRUPTED_ IMPLEMENTATION	T.FLAWED_DESIGN	T.MALICIOUS_TSF_ COMPROMISE	T.MASQUERADE	T.RESIDUAL_DATA	T.RESOURCE_ EXHAUSTION	T.UNATTENDED_ SESSION	T.UNAUTHORIZED_ACCESS	T.UNIDENTIFIED_ ACTIONS
OD.TEST			X								
OD.VULNERABILITY_ ANALYSIS			X	X							
OE.AUDIT_BACKUP	X										
OE.AUDIT_GENERATION											X
OE.AUDIT_REVIEW	X										X
OE.AUDIT_STORAGE	X										
OE.I&A						X					
OE.INACTIVITY									X		
OE.RESIDUAL_INFORMATION							X				
OE.SELFTEST		X			X						
OE.TIME_STAMPS											X
OE.TOE_ACCESS		X			X			X			

4.4.2 Rationale for Threats

Table 4.5 – Threats to Security Objectives Rationale

Threat	Addressed By	Rationale
T.AUDIT_ COMPROMISE A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	**OE.AUDIT_BACKUP** **OE.AUDIT_STORAGE** **OE.AUDIT_REVIEW**	**OE.AUDIT_BACKUP** contributes to mitigating this threat by providing a backup copy of the audit log in case a compromise does occur. **OE.AUDIT_STORAGE** contributes to mitigating this threat by providing secure storage for the audit logs. **OE.AUDIT_REVIEW** helps to mitigate this threat by providing administrators with a mechanism to review the audit logs for activities indicating attempts to violate the security policies.
T.CORRUPT_GRADING	**OD.PARTIAL_SELF_PRO**	**OD.PARTIAL_SELF_PROTECTION**

Threat	Addressed By	Rationale
Malicious users may corrupt the grading algorithm in the TOE to gain financial advantage.	**TECTION** **O.SELFTEST** **O.TOE_ACCESS** **OE.SELFTEST** **OE.TOE_ACCESS**	contributes to mitigating this threat by protecting against tampering and interference through TOE interfaces. **O.SELFTEST** contributes to mitigating this threat by verifying the integrity of the grading algorithm (since it is part of the TOE). **O.TOE_ACCESS** contributes to mitigating this threat by limiting the functions available to TOE users, specifically the ability to modify the TOE. **OE.SELFTEST** contributes to mitigating this threat by verifying the integrity of mechanisms in the IT Environment upon which the TOE is dependent. **OE.TOE_ACCESS** contributes to mitigating this threat by limiting the functions available to IT Environment users, specifically the ability to modify the TOE.
T.CORRUPTED_ IMPLEMENTATION Unintentional or intentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a malicious user or program.	**OD.CONFIGURATION_ IDENTIFICATION** **OD.DELIVERY_INTEGRI TY** **OD.DEVELOPMENT_INT EGRITY** **OD.FLAW_REMEDIATIO N** **OD.TEST** **OD.VULNERABILITY_A NALYSIS**	**OD.CONFIGURATION_IDENTIFICATION** contributes to mitigating this threat by ensuring flaws reported by other users can be correlated to the version of the TOE in use through the unique configuration identification for the version being used. **OD.DELIVERY_INTEGRITY** contributes to mitigating this threat by protecting the integrity of the implementation during delivery to the user. **OD.DEVELOPMENT_INTEGRITY** contributes to mitigating this threat by protecting the integrity of the implementation during the development phase. **OD.FLAW_REMEDIATION** contributes to mitigating this threat by ensuring security vulnerabilities are addressed during and after development of the TOE. **OD.TEST** contributes to mitigating this threat by requiring testing by the vendor and a third party for obvious errors in the implementation. **OD.VULNERABILITY_ANALYSIS** contributes to mitigating this threat by requiring the TOE to undergo vulnerability analysis and penetration testing.
T.FLAWED_DESIGN Unintentional or intentional errors in requirements	**OD.CONFIGURATION_ IDENTIFICATION** **OD.DOCUMENTED_DESI**	**OD.CONFIGURATION_IDENTIFICATION** contributes to mitigating this threat by ensuring flaws reported by other users can

Threat	Addressed By	Rationale
specification or design of the TOE may occur, leading to flaws that may be exploited by a malicious user or program.	**GN** **OD.FLAW_REMEDIATION** **OD.VULNERABILITY_ANALYSIS**	be correlated to the version of the TOE in use through the unique configuration identification for the version being used. **OD.DOCUMENTED_DESIGN** contributes to mitigating this threat by providing details of the design that can be used to in the vulnerability analysis and penetration testing. **OD.FLAW_REMEDIATION** contributes to mitigating this threat by ensuring security vulnerabilities are addressed during and after development of the TOE. **OD.VULNERABILITY_ANALYSIS** contributes to mitigating this threat by requiring the TOE to undergo vulnerability analysis and penetration testing.
T.MALICIOUS_TSF_COMPROMISE A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).	**OD.PARTIAL_SELF_PROTECTION** **O.SELFTEST** **O.TOE_ACCESS** **OE.SELFTEST** **OE.TOE_ACCESS**	**OD.PARTIAL_SELF_PROTECTION** contributes to mitigating this threat by protecting against tampering and interference through TOE interfaces. **O.SELFTEST** contributes to mitigating this threat by verifying the integrity of the TOE. **O.TOE_ACCESS** contributes to mitigating this threat by limiting the functions available to TOE users, specifically the ability to modify the TOE and TOE data. **OE.SELFTEST** contributes to mitigating this threat by verifying the integrity of mechanisms in the IT Environment upon which the TOE is dependent. **OE.TOE_ACCESS** contributes to mitigating this threat by limiting the functions available to IT Environment users, specifically the ability to modify the TOE.
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	**O.TOE_ACCESS** **OE.I&A**	**O.TOE_ACCESS** contributes to mitigating this threat by requiring definition of authorized access for users. **OE.I&A** contributes to mitigating this threat by requiring I&A of users so that the appropriate access limits can be enforced.
T.RESIDUAL_DATA A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.	**OE.RESIDUAL_INFORMATION**	**OE.RESIDUAL_INFORMATION** counters this threat by ensuring that TSF data and user data is not persistent when resources are released by one user/process and allocated to another user/process.

Threat	Addressed By	Rationale
T.RESOURCE_ EXHAUSTION A malicious process or user may block others from system resources (e.g., disk space) via a resource exhaustion denial of service attack.	**O.ACCESS_GRADERS** **O.ACCESS_OPERATORS** **O.ACCESS_PLANTIT** **O.TOE_ACCESS** **OE.TOE_ACCESS**	**O.ACCESS_GRADERS** contributes to mitigating this threat by specifying that Graders are authorized to transfer images from the TOE, releasing disk space for re-use. **O.ACCESS_OPERATORS** contributes to mitigating this threat by specifying that only Operators are permitted to create captured images on the TOE. **O.ACCESS_PLANTIT** contributes to mitigating this threat by specifying that plant IT systems connected to the TOE are limited in the information flows permitted with them. No image transfers to the TOE may occur via these connections. **O.TOE_ACCESS** contributes to mitigating this threat by requiring definition of authorized access for TOE users. Operators are the only users authorized to create captured images, which are the primary consumer of disk space. **OE.TOE_ACCESS** contributes to mitigating this threat by requiring definition of authorized access for IT Environment users. No non-TOE users are authorized to consume disk space.
T.UNATTENDED_ SESSION A user may gain unauthorized access to an unattended session.	**O.INACTIVITY** **OE.INACTIVITY**	**O.INACTIVITY** contributes to mitigating this threat by requiring the TOE to terminate sessions that are inactive for longer than the configured inactivity time. **OE.INACTIVITY** contributes to mitigating this threat by requiring the IT Environment to terminate sessions that are inactive for longer than the configured inactivity time.
T.UNAUTHORIZED_ACCESS A user may gain access to user data for which they are not authorized according to the TOE security policy.	**O.MEDIATE**	**O.MEDIATE** ensures that all accesses to user data are subject to mediation. The TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content.
T.UNIDENTIFIED_ ACTIONS The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action	**O.AUDIT_GENERATION** **OE.AUDIT_GENERATION** **OE.AUDIT_REVIEW** **OE.TIME_STAMPS**	**O.AUDIT_GENERATION** helps to mitigate this threat by recording actions of TOE users for later review. **OE.AUDIT_GENERATION** helps to mitigate this threat by recording actions of IT Environment users for later review.

Threat	Addressed By	Rationale
against a possible security breach.		**OE.AUDIT_REVIEW** helps to mitigate this threat by providing administrators with a mechanism to review the audit logs for activities indicating attempts to violate the security policies. **OE.TIME_STAMPS** helps to mitigate this threat by ensuring that audit records have correct timestamps.

4.4.3 Mapping of Policies to Objectives

The following table presents a mapping of the policies to the objectives defined in this PP. Only objectives that map to one or more of the policies is included in this table.

Table 4.6 – Mapping of Policies to Objectives

	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.ADMIN_ACCESS	P.DATA_DELIVERY	P.I_AND_A	P.ROLES	P.SYSTEM_INTEGRITY	P.VULNERABILITY_ ANALYSIS_TEST
O.ACCESS_GRADERS				X		X		
O.ACCESS_TECHNICIANS						X		
O.ACCESS_VENDORS						X		
O.AUDIT_GENERATION		X						
O.DATA_DELIVERY				X				
O.DATA_PROTECTION				X				
O.DATA_STORAGE				X				
O.DISPLAY_BANNER	X							
O.MANAGE			X					
O.SELFTEST							X	
O.TOE_ACCESS		X						
OD.VULNERABILITY_ANALYSIS								X
OE.ACCESS_REVIEWERS				X				
OE.ACCESS_SYSADMINS						X		

	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.ADMIN_ACCESS	P.DATA_DELIVERY	P.I_AND_A	P.ROLES	P.SYSTEM_INTEGRITY	P.VULNERABILITY_ ANALYSIS_TEST
OE.AUDIT_REVIEW		X						
OE.DATA_PROTECTION				X				
OE.DISPLAY_BANNER	X							
OE.I&A					X			
OE.SECURE_COMMS			X					
OE.SELFTEST							X	
OE.TIME_STAMPS		X						

4.4.4 Rationale for Policies

Table 4.7 – Policies to Security Objectives Rationale

Policy	Addressed By	Rationale
P.ACCESS_BANNER The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which administrators consent by accessing the system.	**O.DISPLAY_BANNER** **OE.DISPLAY_BANNER**	**O.DISPLAY_BANNER** satisfies this policy by ensuring that the TOE displays a Security Administrator configurable banner that provides all interactive users with a warning about the unauthorized use of the TOE. **OE.DISPLAY_BANNER** satisfies this policy by ensuring that the IT Environment displays a Security Administrator configurable banner that provides all interactive users with a warning about the unauthorized use of the IT Environment.
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	**O.AUDIT_GENERATION** **O.TOE_ACCESS** **OE.TIME_STAMPS** **OE.AUDIT_REVIEW**	**O.AUDIT_GENERATION** addresses this policy by providing the capability to record the actions performed by users, or review the audit trail which includes the identity of the user. Additionally, the administrator's ID is recorded when any security relevant change is made to the TOE or IT Environment.

Policy	Addressed By	Rationale
		O.TOE_ACCESS supports this policy by requiring the TOE to identify and authenticate all authorized users prior to allowing any TOE access or any TOE mediated access on behalf of those users. **OE.TIME_STAMPS** plays a role in supporting this policy by requiring the IT Environment to provide a reliable time stamp. The audit mechanism is required to include the current date and time in each audit record. All audit records that include the user ID, will also include the date and time that the event occurred. **OE.AUDIT_REVIEW** helps to mitigate this threat by providing administrators with a mechanism to review the audit logs for activities indicating attempts to violate the security policies.
P.ADMIN_ACCESS Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.	**O.MANAGE** **OE.SECURE_COMMS**	**O.MANAGE** supports this policy by requiring the TOE to provide the required management functions to the administrative roles. **OE.SECURE_COMMS** supports this policy by requiring the IT Environment to secure communications between the TOE and remote administrators.
P.DATA_DELIVERY The TOE shall maintain captured and processed images used in calculating the grades and data records reflecting the grades until delivered to a USDA Grader.	**O.ACCESS_GRADERS** **O.DATA_DELIVERY** **O.DATA_PROTECTION** **O.DATA_STORAGE** **OE.ACCESS_REVIEWERS** **OE.DATA_PROTECTION**	**O.ACCESS_GRADERS** supports this policy by requiring that Graders be able to initiate the data delivery process. **O.DATA_DELIVERY** addresses this policy by requiring the TOE to provide a mechanism to deliver the images and data records to a Grader. **O.DATA_PROTECTION** addresses this policy by requiring the TOE to protect the stored images and data records until they are delivered to a Grader. **O.DATA_STORAGE** addresses this policy by requiring the TOE to store the images and data records until they have delivered to a Grader. **OE.ACCESS_REVIEWERS** supports this policy by limiting Reviewer access to the stored images to view only. Therefore, those users can't modify or delete the stored information before it is delivered to the Graders. **OE.DATA_PROTECTION** addresses this

Policy	Addressed By	Rationale
		policy by requiring the IT Environment to protect the stored images and data records until they are delivered to a Grader.
P.I_AND_A All users must be identified and authenticated prior to accessing any controlled resources with the exception of public objects.	**OE.I&A**	**OE.I&A** satisfies this policy by requiring the IT Environment to perform the I&A function for all users.
P.ROLES The TOE shall provide authorized administrator roles for secure administration of the TOE. These roles shall be separate and distinct from other authorized users.	**O.ACCESS_GRADERS** **O.ACCESS_TECHNICIANS** **O.VENDORS** **OE.ACCESS_SYSADMINS**	**O.ACCESS_GRADERS, O.ACCESS_TECHNICIANS, O.VENDORS**, and **OE.ACCESS_SYSADMINS** satisfy this policy by defining the administrative roles for the TOE and IT Environment.
P.SYSTEM_INTEGRITY The TOE shall provide the ability to periodically validate its correct operation.	**O.SELFTEST** **OE.SELFTEST**	**O.SELFTEST** partially satisfies this policy by requiring functionality in the TOE to validate the integrity of the TOE. Since the TOE is software only, it is sufficient to verify a hash of the TOE. **OE.SELFTEST** partially satisfies this policy by verifying the integrity of mechanisms in the IT Environment upon which the TOE is dependent.
P.VULNERABILITY_ ANALYSIS_TEST The TOE must undergo appropriate independent vulnerability analysis and penetration testing to demonstrate that the TOE is resistant to an attacker possessing a basic attack potential.	**OD.VULNERABILITY_ANALYSIS**	**OD.VULNERABILITY_ANALYSIS** satisfies this policy by requiring vulnerability analysis and penetration testing of the TOE.

4.4.5 Mapping of Assumptions to Objectives

The following table presents a mapping of the assumptions to the objectives defined in this PP. Only objectives that map to one or more of the assumptions is included in this table.

Table 4.8 – Mapping of Assumptions to Objectives

	A.MANAGE	A.NETWORK_ACCESS	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.ROBUST_ENVIRONMENT	A.SECURE_COMMS	A.TRAINED_ADMINISTRATORS	A.TRUSTED_INDIVIDUAL
OD.ADMIN_GUIDANCE	X				X		X	
OE.DEDICATED_SYSTEMS			X					
OE.NETWORK_ACCESS		X						
OE.NO_EVIL	X						X	X
OE.PHYSICAL_ACCESS				X				
OE.SECURE_COMMS						X		
OE.TRUST_IT					X			

4.4.6 Rationale for Assumptions

Table 4.9 – Assumptions to Security Objectives Rationale

Assumption	Addressed By	Rationale
A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	**OD.ADMIN_GUIDANCE** **OE.NO_EVIL**	**OD.ADMIN_GUIDANCE** supports this assumption by ensuring adequate guidance documentation for the TOE is available. **OE.NO_EVIL** addresses this assumption by ensuring an appropriately trained, non-hostile administrator is available to follow the guidance documentation while managing the TOE.
A.NETWORK_ACCESS Administrators will limit network access to the TOE and TOE data to authorized users with valid requirements for network access to the TOE.	**OE.NETWORK_ACCESS**	**OE.NETWORK_ACCESS** addresses this assumption by requiring the network to be configured to restrict network assess to the TOE to the greatest extent possible.
A.NO_GENERAL_PURPOSE The administrator ensures there are no general-purpose computing or storage	**OE.DEDICATED_SYSTEMS**	**OE.DEDICATED_SYSTEMS** addresses this assumption by requiring the systems on which the TOE executes to be dedicated to the TOE.

Assumption	Addressed By	Rationale
repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.		
A.PHYSICAL It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.	**OE.PHYSICAL_ACCESS**	**OE.PHYSICAL_ACCESS** addresses this assumption by requiring controlled physical access to the systems on which the TOE is executing.
A.ROBUST_ENVIRONMENT It is assumed that the IT environment is at least as robust as the TOE.	**OD.ADMIN_GUIDANCE** **OE.TRUST_IT**	**OD.ADMIN_GUIDANCE** supports this assumption by providing guidance documentation that communicates the security requirements of the TOE. **OE.TRUST_IT** addresses this assumption by requiring the systems on which the TOE is installed to be installed and managed consistent with the security requirements of the TOE.
A.SECURE_COMMS It is assumed that the IT environment will provide secure communications between remote users and the IGS, and between distributed components of the TOE.	**OE.SECURE_COMMS**	**OE.SECURE_COMMS** addresses this assumption by requiring the IT Environment to ensure secure communications between distributed TOE components and between the TOE and remote users.
A.TRAINED_ADMINISTRATORS Authorized administrators (users with the Technician, Vendor or SysAdmin role) are appropriately trained and follow all administrator guidance	**OD.ADMIN_GUIDANCE** **OE.NO_EVIL**	**OD.ADMIN_GUIDANCE** supports this assumption by ensuring adequate guidance documentation for the TOE is available. **OE.NO_EVIL** addresses this assumption by ensuring an appropriately trained, non-hostile administrator is available to follow the guidance documentation while managing the TOE.
A.TRUSTED_INDIVIDUAL If an individual is allowed to perform procedures upon which the security of the TOE may depend, it is assumed that the individual is trusted with assurance commensurate with the value of the IT assets.	**OE.NO_EVIL**	**OE.NO_EVIL** addresses this assumption by ensuring a non-hostile administrator is available to manage the TOE.

5 Extended Components Definition

This section provides the definition of any extended components used in the PP.

The only extended components used in this PP derive from NIAP interpretations to the standard SFRs and one extended component defined in [BRCIM]. In all cases, the dependencies and hierarchies of the extended SFRs are identical to the SFRs from which they are derived. In addition, the audit requirements and management action recommendations associated with the extended components are the same as for the standard SFRs from which they are derived.

The following table details the extended components, the SFRs from which they are derived, and the associated NIAP interpretation.

Table 5.1 – Extended Component Details

Extended Component	SFR Derived From	NIAP Interpretation
FAU_GEN.1-NIAP-0407	FAU_GEN.1	I-0407: Empty Selections Or Assignments
FAU_GEN.2-NIAP-0410	FAU_GEN.2	I-0410: Auditing Of Subject Identity For Unsuccessful Logins
FDP_ACF.1-NIAP-0407	FDP_ACF.1	I-0407: Empty Selections Or Assignments
FDP_IFF.1-NIAP-0407	FDP_IFF.1	I-0407: Empty Selections Or Assignments
FPT_TST_EXT.1	FPT_TST.1	n/a

5.1 FAU_GEN.1-NIAP-0407 Audit Data Generation

FAU_GEN.1.1-NIAP-0407 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 listed in Table x;

c) [selection: [assignment: *events at a basic level of audit introduced by the inclusion of additional SFRs determined by the ST author*], [assignment: *events commensurate with a basic level of audit introduced by the inclusion of extended requirements determined by the ST author*], "*no additional events*"].

FAU_GEN.1.2-NIAP-0407 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 (if applicable), 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,

[selection: [assignment: *other audit relevant information, excluding sensitive fields], "no other information"*].

5.2 FAU_GEN.2-NIAP-0410 User Identity Association

FAU_GEN.2.1-NIAP-0410 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.3 FDP_ACF.1-NIAP-0407 Security Attribute Based Access Control

FDP_ACF.1.1-NIAP-0407 The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes or named groups of SFP-relevant security attributes*].

FDP_ACF.1.2-NIAP-0407 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

FDP_ACF.1.3-NIAP-0407 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [selection: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects],"no additional rules"*].

FDP_ACF.1.4-NIAP-0407 The TSF shall explicitly deny access of subjects to objects based on the following rules: [selection: [assignment: *rules, based on security attribute, that explicitly deny access of subjects to objects], "no additional explicit denial rules"*].

5.4 FDP_IFF.1-NIAP-0407 Simple Security Attributes

FDP_IFF.1.1-NIAP-0407 The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *list of subjects and information controlled under the indicated SFP, and, for each, the security attributes*].

FDP_IFF.1.2-NIAP-0407 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security-attribute based relationship that must hold between subject and information security attributes*].

FDP_IFF.1.3-NIAP-0407 The TSF shall enforce the following information flow control rules: [selection: [assignment: *additional information flow control SFP rules], "no additional information flow control SFP rules"*].

FDP_IFF.1.4-NIAP-0407 The TSF shall provide the following [selection: [assignment: *list of additional SFP capabilities], "no additional SFP capabilities"*].

FDP_IFF.1.5-NIAP-0407 The TSF shall explicitly authorise an information flow based upon the following rules: [selection: [assignment: *rules, based on security attributes, that explicitly authorise information flows], "no explicit authorisation rules"*].

FDP_IFF.1.6-NIAP-0407 The TSF shall explicitly deny an information flow based upon the following rules: [selection: [assignment: *rules, based on security attributes, that explicitly deny information flows], "no explicit denial rules"*].

5.5 FPT_TST_EXT.1 TSF Testing for Software TOEs

FPT_TST_EXT.1.1 The TSF shall provide administrator with the capability to verify the integrity of the following TSF data: [assignment: *TSF data for which integrity validation is required*].

FPT_TST_EXT.1.2 The TSF shall provide administrator with the capability to verify the integrity of stored TSF executable code.

This extended SFR addresses 2 concerns with FPT_TST.1. First, the wording of FPT_TST.1.1 appears to make sense only if the TOE includes hardware; it is difficult to imagine what software TSF "self-tests" would be run. Secondly, some TOE data are dynamic (e.g., data in the audit trail, passwords) and so interpretation of "integrity" for FPT_TST.1.2 is required, leading to potential inconsistencies amongst Basic Robustness TOEs.

6 IT Security Requirements

This section provides the TOE security functional and assurance requirements that must be satisfied by a Protection Profile-compliant TOE, and the IT environment security functional requirements on which the TOE relies. These requirements consist of functional components from Part 2 of the CC, assurance components from Part 3 of the CC, Common Criteria interpretations, NIAP interpretations, and extended functional components derived from the CC components.

6.1 TOE Security Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1-NIAP-0407(1) Audit Data Generation

FAU_GEN.1.1-NIAP-0407(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 listed in Table 6.1;

c) *events at a basic level of audit introduced by the inclusion of additional SFRs determined by the ST author*;

d) *events commensurate with a basic level of audit introduced by the inclusion of extended requirements determined by the ST author*.

FAU_GEN.1.2-NIAP-0407(1) 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 (if applicable), 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, *the additional audit record contents shown in the Table 6.1*.

Table 6.1 – FAU_GEN.1(1) Details

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1-NIAP-0407	None	
FAU_GEN.2-NIAP-0410	None	
FDP_ACC.1	None	
FDP_ACF.1-NIAP-0407	All modify, transfer and delete operations	Carcass ID, override grade (if applicable)

Requirement	Auditable Events	Additional Audit Record Contents
FIA_AFL.1	Reaching the threshold for the unsuccessful authentication attempts	Source of the attempts (e.g., specific terminal), the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).
FIA_ATD.1	Rejection or acceptance by the TSF of any tested secret	
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret	
FIA_UAU.2	All use of the authentication mechanism	Source of the login
FIA_UID.2	All use of the identification mechanism	Source of the login
FIA_USB.1	Failure to create a subject	
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	Version identifier for the code installed
FMT_MSA.1	All modifications of the values of security attributes	Security attributes modified, new value, userid associated with the security attribute
FMT_MSA.3	All modifications of the initial values of security attributes	Assigned role, userid associated with the role
FMT_MTD.1	All modifications to the values of TSF data	Parameter and new value (except for the security banner)
FMT_SMF.1	None	
FMT_SMR.1	Modifications to the group of users that are part of a role	Role and userid(s)
FPT_TST_EXT.1	Execution of the TSF tests	Results of the tests
FTA_SSL.3	Termination of an interactive session by the session locking mechanism	Userid and type of the session terminated
FTA_TAB.1	None	

6.1.1.2 FAU_GEN.2-NIAP-0410(1) User Identity Association

FAU_GEN.2.1-NIAP-0410(1) For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.2 User Data Protection (FDP)

6.1.2.1 FDP_ACC.1(1) Subset Access Control

FDP_ACC.1.1(1) The TSF shall enforce the User Access Control SFP on

a) subjects: TOE components providing access to users of the TOE;

b) objects: captured and processed images, carcass parameters, and data records (including carcass identifiers and grades)

c) operations: create, view, replace, correlate, modify, transfer, delete.

Application Note: The "replace" operation applies to the situation where a captured image is of insufficient quality and the imaging process must be repeated before the carcass can be properly graded. The "correlate" operation refers to the correlation of carcass identifiers with images, so that the TOE may combine data from each to calculate a grade and produce a corresponding data record; correlation is performed by the Operators, typically by specifying a carcass ID to the TOE for the image being created. The "transfer" operation refers to the transfer of a copy of the official records (the objects) to the USDA (a Grader); the data under the TOE's control may not be deleted until a copy has been transferred to the USDA.

6.1.2.2 FDP_ACF.1-NIAP-0407(1) Security Attribute Based Access Control

FDP_ACF.1.1-NIAP-0407(1) The TSF shall enforce the User Access Control SFP to objects based on the following:

a) subject security attributes: role;

b) object security attributes: transfer status.

FDP_ACF.1.2-NIAP-0407(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: as specified in the following table.

Table 6.2 – User Access Control SFP Details

Data Operation	Captured Images	Carcass Parameters	Data Records
Create	Operators	PlantIT	None (performed automatically by the TOE)
View	Grader, Operator, Technician, Vendor	Technician, Vendor	Operator, Grader, PlantIT, Technician, Vendor
Replace	Operators (only before the corresponding carcass has been graded)	None	None

Data Operation	Captured Images	Carcass Parameters	Data Records
Correlate	Operators (only before the corresponding carcass has been graded)	None	None
Modify	None	None	Graders (may override the calculated grade)
Transfer	Graders	None	Graders
Delete	Technicians, Vendors (the TOE may also perform this operation automatically)	Technicians, Vendors (the TOE may also perform this operation automatically)	Technicians, Vendors (the TOE may also perform this operation automatically)

FDP_ACF.1.3-NIAP-0407(1) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [selection: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects],"no additional rules"*].

FDP_ACF.1.4-NIAP-0407(1) The TSF shall explicitly deny access of subjects to objects based on the following rules:

a) *Captured images and data records may not be deleted by any role until the information has been transferred by a Grader.*

b) [selection: [assignment: *rules, based on security attribute, that explicitly deny access of subjects to objects], "no additional explicit denial rules"*].

Application Note: Any additional rules enforced by a TOE that explicitly authorize or deny access should be listed by the ST author.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: *positive integer number*], *"an administrator configurable positive integer within [assignment: range of acceptable values]"*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

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

Application Note: A conformant TOE may choose between a fixed or dynamically configurable number. Failure hanlding will be factored into the evaluation of the authentication mechanism, which must satisfy the requirements

of AVA_VAN.2. If a configurable number is supported, the evaluation of the mechanism must assume the worst case.

Application Note: If the number of consecutive login failures triggering further action is configurable, permissions to view or change the parameter should be addressed in FMT_MTD.

6.1.3.2 FIA_ATD.1 User Attribute Definition

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

Application Note: It is not required that a common database of userids be maintained with roles explicitly associated with each userid. Conforming products may implement multiple special-purpose device types, one per role, with separate authentication databases for each. The role could be implied by the database against which authentication occurred.

6.1.3.3 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

Application Note: In the ST, the vendor is required to state the strength of the metric enforced by the TOE for any implemented mechanism(s). The overall strength is determined by the enforced mechanism(s) together with guidance provided to administrators for elements under their control (i.e., not chosen by the users). The overall strength must satisfy (at a minimum) the requirement of AVA_VAN.2 that the TOE is resistant to an attacker with attack potential Basic.

6.1.3.4 FIA_UAU.2 User Authentication Before any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: Communication with the PlantIT role is commonly performed over a dedicated connection between the systems. Under those circumstances, authentication is implied by the dedicated connection.

6.1.3.5 FIA_UID.2 User Identification Before any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note: Communication with the PlantIT role is commonly performed over a dedicated connection between the systems. Under those circumstances, identification is implied by the dedicated connection.

6.1.3.6 FIA_USB.1 User-Subject Binding

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

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: the role is determined from the security attributes associated with the userid on whose behalf the subject is executing.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: once associated, the role may not change during a session.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to *modify the behaviour of* the functions grading to Vendors.

Application Note: The grading algorithm is embedded within the executable code of the TOE, so it's behavior can only be modified by updating the executable code. Only vendors may update the executable code. Note that updating the executable may take the TOE out of an evaluated configuration.

6.1.4.2 FMT_MSA.1(1) Management of Security Attributes

FMT_MSA.1.1(1) The TSF shall enforce the User Access Control SFP to restrict the ability to *change_default, query, modify, delete* the security attributes Operator, PlantIT, and Technician login credentials to Technicians.

Application Note: If communication with the PlantIT systems occurs over a dedicated connection, login credentials are not required for that role.

6.1.4.3 FMT_MSA.1(2) Management of Security Attributes

FMT_MSA.1.1(2) The TSF shall enforce the User Access Control SFP to restrict the ability to *change_default, query, modify, delete* the security attributes Grader and Vendor login credentials to Vendors.

6.1.4.4 FMT_MSA.3(1) Static Attribute Initialisation

FMT_MSA.3.1(1) The TSF shall enforce the User Access Control SFP to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the Technicians and Vendors to specify alternative initial values to override the default values when an object or information is created.

6.1.4.5 FMT_MTD.1(1) Management of TSF Data

FMT_MTD.1.1(1) The TSF shall restrict the ability to *change_default, query, modify* the camera parameters, communication parameters for other systems, security banner to Technicians.

6.1.4.6 FMT_MTD.1(2) Management of TSF Data

FMT_MTD.1.1(2) The TSF shall restrict the ability to *change_default, query, modify* the inactivity timers for sessions to Vendors.

6.1.4.7 FMT_SMF.1(1) Specification of Management Functions

FMT_SMF.1.1(1) The TSF shall be capable of performing the following management functions:

a) updating the TOE executable code,

b) configuring access credentials,

c) configuring camera parameters

d) configuring communication parameters for communication with other systems (e.g., Plant IT systems)

e) configuring the security banner displayed at the beginning of interactive sessions

f) configuring the inactivity timer for interactive sessions

g) [selection: [assignment: *other functions]*, "*no additional functions"*].

Application Note: If any management functions are added, additions to SFRs (e.g. FMT_MOF.1) may also be required.

6.1.4.8 FMT_SMR.1(1) Security Roles

FMT_SMR.1.1(1) The TSF shall maintain the roles Grader, Operator, PlantIT, Technician, Vendor, [selection: [assignment: *other authorised identified roles]*, "*no additional roles"*].

FMT_SMR.1.2(1) The TSF shall be able to associate users with roles.

Application Note: If additional roles are specified, they must only be refinements of the already defined roles. For example, multiple levels of Technicians may be defined, and none of them may have greater privileges than the single Technician role already defined.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_TST_EXT.1 TSF Testing for Software TOEs

FPT_TST_EXT.1.1 The TSF shall provide the administrator with the capability to verify the integrity of the following TSF data: all TSF data instantiating the grading algorithm, [selection: [assignment: other *TSF data for which integrity validation is required*], "*no additional TSF data*"].

FPT_TST_EXT.1.2 The TSF shall provide administrator with the capability to verify the integrity of stored TSF executable code.

Application Note: If any portion of the grading algorithm is instantiated via TSF data (i.e., parameters which could be changed without updating the executable code), the integrity of those items must be verified. If the algorithm is entirely instantiated in the executable code, then this element is considered satisfied. If a TOE verifies the integrity of other TSF data, the ST author should identify those items.

6.1.6 TOE Access (FTA)

6.1.6.1 FTA_SSL.3(1) TSF-Initiated Termination

FTA_SSL.3.1(1) The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].

Application Note: The time interval may be fixed or configurable. If it is configurable, permissions to view or change the parameter should be addressed in FMT_MTD.

6.1.6.2 FTA_TAB.1(1) Default TOE Access Banners

FTA_TAB.1.1(1) Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

6.2 Security requirements for the IT Environment

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1-NIAP-0407(2) Audit Data Generation

FAU_GEN.1.1-NIAP-0407(2) The **IT Environment** 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 listed in Table 6.3;

c) *events at a basic level of audit introduced by the inclusion of additional SFRs determined by the ST author*;

d) *events commensurate with a basic level of audit introduced by the inclusion of extended requirements determined by the ST author*.

FAU_GEN.1.2-NIAP-0407(2) The **IT Environment** shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), 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, *the additional audit record contents shown in the Table 6.3*.

Table 6.3 – FAU_GEN.1(2) Details

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1-NIAP-0407	None	
FAU_GEN.2-NIAP-0410	None	
FAU_SAR.1	None	
FAU_SAR.2	None	
FAU_STG.1	None	
FDP_ACC.1	None	
FDP_ACF.1-NIAP-0407	All modify, transfer and delete operations	Carcass ID, override grade (if applicable)
FDP_IFC.1	None	
FDP_IFF.1-NIAP-0407	All datagrams filtered	Source and destination address of the traffic
FDP_RIP.1	None	

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UAU.1	All use of the authentication mechanism	Source of the login
FIA_UID.1	All use of the identification mechanism	Source of the login
FMT_MSA.1	All modifications of the values of security attributes	Security attributes modified, new value, userid associated with the security attribute
FMT_MSA.3	All modifications of the initial values of security attributes	Assigned role, userid associated with the role
FMT_MTD.1	All modifications to the values of TSF data	Parameter and new value (except for the security banner)
FMT_SMF.1	None	
FMT_SMR.1	Modifications to the group of users that are part of a role	Role and userid(s)
FPT_AMT.1	Execution of the tests	Results of the tests
FPT_STM.1	None	
FTA_SSL.3	Termination of an interactive session by the session locking mechanism	Userid and type of the session terminated
FTA_TAB.1	None	
FTP_ITC.1	Any failure to establish a secure connection	Details of the attempted connection and reason for failure

6.2.1.2 FAU_GEN.2-NIAP-0410(2) User Identity Association

FAU_GEN.2.1-NIAP-0410(2) For audit events resulting from actions of identified users, the **IT Environment** shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The **IT Environment** shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.

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

6.2.1.4 FAU_SAR.2 Restricted Audit Review

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

6.2.1.5 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The **IT Environment** shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The **IT Environment** shall be able to *prevent* unauthorised modifications to the audit records in the audit trail.

6.2.2 User Data Protection (FDP)

6.2.2.1 FDP_ACC.1(2) Subset Access Control

FDP_ACC.1.1(2) The **IT Environment** shall enforce the ITEnv User Access SFP on

a) subjects: software outside the TSC on the IT systems on which the TOE is installed providing access to data on those IT systems;

b) objects: captured and processed images, carcass parameters, and data records (including carcass identifiers and grades)

c) operations: create, view, replace, correlate, modify, transfer, delete.

6.2.2.2 FDP_ACF.1-NIAP-0407(2) Security Attribute Based Access Control

FDP_ACF.1.1-NIAP-0407(2) The **IT Environment** shall enforce the ITEnv User Access SFP to objects based on the following:

a) subject security attributes: role;

b) object security attributes: none.

FDP_ACF.1.2-NIAP-0407(2) The **IT Environment** shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Table 6.4 – ITEnv User Access Control SFP Details

Data Operation	Captured Images	Carcass Parameters	Data Records
Create	None	None	None
View	Reviewer	None	None
Replace	None	None	None
Correlate	None	None	None
Modify	None	None	None
Transfer	None	None	None
Delete	None	None	None

FDP_ACF.1.3-NIAP-0407(2) The **IT Environment** shall explicitly authorise access of subjects to objects based on the following additional rules: *no additional rules*.

FDP_ACF.1.4-NIAP-0407(2) The **IT Environment** shall explicitly deny access of subjects to objects based on the following rules: *any access operation not described in other elements is denied*.

6.2.2.3 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The **IT Environment** shall enforce the Grading System Access SFP on

a) subjects: network interfaces of firewalls interconnecting the LAN on which the TOE is installed with other LANs;

b) information: network traffic sent to or from an IT system on which the TOE is installed;

c) operations: forward network traffic.

6.2.2.4 FDP_IFF.1-NIAP-0407 Simple Security Attributes

FDP_IFF.1.1-NIAP-0407 The **IT Environment** shall enforce the Grading System Access SFP based on the following types of subject and information security attributes:

a) subjects: none;

b) information: presumed source address specified in the traffic, presumed destination address specified in the traffic.

FDP_IFF.1.2-NIAP-0407 The **IT Environment** shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) If the presumed destination address is a system on which the TOE is installed, the traffic is forwarded only if the presumed source address is authorized to communicate with the TOE.

b) If the presumed source address is a system on which the TOE is installed, the traffic is forwarded only if the presumed destination address is authorized to communicate with the TOE.

Application Note: Authorization is determined by the administrators of the plant IT systems.

FDP_IFF.1.3-NIAP-0407 The **IT Environment** shall enforce the following information flow control rules: *no additional information flow control SFP rules*.

FDP_IFF.1.4-NIAP-0407 The **IT Environment** shall provide the following *no additional SFP capabilities.*

FDP_IFF.1.5-NIAP-0407 The **IT Environment** shall explicitly authorise an information flow based upon the following rules: *no explicit authorisation rules*.

FDP_IFF.1.6-NIAP-0407 The **IT Environment** shall explicitly deny an information flow based upon the following rules: *any information flows to or from a system on which the TOE is installed is denied unless the other endpoint is an authorized system.*

6.2.2.5 FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1 The **IT Environment** shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, de-allocation of the resource from*] the following objects: memory used by processes instantiating the TOE and [selection: [assignment: *list of other objects*], "*no other objects*"].

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_UAU.1 Timing of Authentication

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

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

6.2.3.2 FIA_UID.1 Timing of Identification

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

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

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MSA.1(3) Management of Security Attributes

FMT_MSA.1.1(3) The **IT Environment** shall enforce the ITEnv User Access SFP to restrict the ability to *change_default, query, modify, delete* the security attributes login credentials used by the IT Environment to SysAdmins.

6.2.4.2 FMT_MSA.3(2) Static Attribute Initialisation

FMT_MSA.3.1(2) The **IT Environment** shall enforce the User Access Control SFP to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The **IT Environment** shall allow the SysAdmins to specify alternative initial values to override the default values when an object or information is created.

6.2.4.3 FMT_MTD.1(3) Management of TSF Data

FMT_MTD.1.1(3) The **IT Environment** shall restrict the ability to *modify* the network access parameters, system time, inactivity timers, and security banners to SysAdmins.

Application Note: This SFR refers to the system time maintained on an IT system on which the TOE is installed.

6.2.4.4 FMT_SMF.1(2) Specification of Management Functions

FMT_SMF.1.1(2) The **IT Environment** shall be capable of performing the following management functions:

a) configuring access credentials,

b) configuring network access parameters

c) configuring the system time

d) configuring the security banner displayed at the beginning of interactive sessions

e) configuring the inactivity timer for interactive sessions

f) [selection: [assignment: *other functions]*, *"no additional functions"*].

6.2.4.5 FMT_SMR.1(2) Security Roles

FMT_SMR.1.1(2) The **IT Environment** shall maintain the roles Reviewer, SysAdmin, [selection: [assignment: *other authorised identified roles*], "*no other roles*"].

FMT_SMR.1.2(2) The **IT Environment** shall be able to associate users with roles.

6.2.5 Protection of the TSF (FPT)

6.2.5.1 FPT_AMT.1 Abstract Machine Testing

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

Application Note: Testing must be performed at start-up, and may be performed at other times.

6.2.5.2 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The **IT Environment** shall be able to provide reliable time-stamps.

6.2.6 TOE Access (FTA)

6.2.6.1 FTA_SSL.3(2) TSF-Initiated Termination

FTA_SSL.3.1(2) The **IT Environment** shall terminate an interactive session after a [assignment: *time interval of user inactivity*].

6.2.6.2 FTA_TAB.1(2) Default TOE Access Banners

FTA_TAB.1.1(2) Before establishing a user session, the **IT Environment** shall display an advisory warning message regarding unauthorised use of the TOE.

6.2.7 Trusted Path/Channels (FTP)

6.2.7.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The **IT Environment** 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 channel data from modification or disclosure.

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

FTP_ITC.1.3 The **IT Environment** shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

Application Note: The trusted channel is intended to be used for any communication in which a password would be transferred (to prevent the transfer in clear text) or for any communication involving data that should not be disclosed or modified per the security policies stated in the PP. The TOE is responsible for setting up the configuration parameters for the communication (FMT_MTD.1(1)) and the IT Environment is responsible for facilitating the communication.

6.3 TOE Security Assurance Requirements

The TOE assurance requirements for this PP are EAL2 augmented by ALC_FLR.2. The assurance requirements are summarized in the following table.

Table 6.5 – Assurance Requirements

Assurance Class	Assurance Components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life Cycle Support	ALC_CMC.2	Use of a CM system

Assurance Class	Assurance Components	
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.4 TOE Security Functional Requirements Rationale

6.4.1 Mapping of TOE Objectives to SFRs

The following table presents a mapping of the objectives to the SFRs levied on the TOE in this PP.

Table 6.6 – Mapping of TOE Objectives to SFRs

	O.ACCESS_GRADERS	O.ACCESS_OPERATORS	O.ACCESS_PLANTIT	O.ACCESS_TECHNICIANS	O.ACCESS_VENDORS	O.AUDIT_GENERATION	O.DATA_DELIVERY	O.DATA_PROTECTION	O.DATA_STORAGE	O.DISPLAY_BANNER	O.INACTIVITY	O.MANAGE	O.MEDIATE	O.SELFTEST	O.TOE_ACCESS
FAU_GEN.1-NIAP-0407(1)						X									
FAU_GEN.2-NIAP-0410(1)						X									
FDP_ACC.1(1)	X	X	X	X	X		X	X	X				X		X
FDP_ACF.1-NIAP-0407(1)	X	X	X	X	X		X	X	X				X		X
FIA_AFL.1															X
FIA_ATD.1															X
FIA_SOS.1															X
FIA_UAU.2	X	X		X	X										X

	O.ACCESS_GRADERS	O.ACCESS_OPERATORS	O.ACCESS_PLANTIT	O.ACCESS_TECHNICIANS	O.ACCESS_VENDORS	O.AUDIT_GENERATION	O.DATA_DELIVERY	O.DATA_PROTECTION	O.DATA_STORAGE	O.DISPLAY_BANNER	O.INACTIVITY	O.MANAGE	O.MEDIATE	O.SELFTEST	O.TOE_ACCESS
FIA_UID.2	X	X		X	X										X
FIA_USB.1															X
FMT_MOF.1					X										X
FMT_MSA.1(1)				X											X
FMT_MSA.1(2)					X										X
FMT_MSA.3(1)				X	X										X
FMT_MTD.1(1)				X											X
FMT_MTD.1(2)					X										X
FMT_SMF.1(1)												X			X
FMT_SMR.1(1)												X			X
FPT_TST_EXT.1														X	
FTA_SSL.3											X				
FTA_TAB.1										X					

6.4.2 Rationale for TOE Objectives

Table 6.7 – TOE Security Objectives to SFRs Rationale

Objective	Addressed By	Rationale
O.ACCESS_GRADERS	FDP_ACC.1(1) FDP_ACF.1-NIAP-0407(1) FIA_UAU.2 FIA_UID.2	**FDP_ACC.1(1) and FDP_ACF.1-NIAP-0407(1)** – These SFRs address the objective by specifying that Graders have view access to images and records, modify access to records, and transfer access to images and records. **FIA_UAU.2 and FIA_UID.2** – These SFRs address the objective by specifying that the TOE provide I&A functions.
O.ACCESS_OPERATORS	FDP_ACC.1(1) FDP_ACF.1-NIAP-	**FDP_ACC.1(1) and FDP_ACF.1-NIAP-0407(1)** – These SFRs address the objective by specifying that

Objective	Addressed By	Rationale
	0407(1) FIA_UAU.2 FIA_UID.2	Operators have create access to images, view access to images and records, correlate access to images and replace access to images. **FIA_UAU.2 and FIA_UID.2** – These SFRs address the objective by specifying that the TOE provide I&A functions.
O.ACCESS_PLANTIT	FDP_ACC.1(1) FDP_ACF.1-NIAP-0407(1)	**FDP_ACC.1(1) and FDP_ACF.1-NIAP-0407(1)** - These SFRs address the objective by specifying that PlantIT have create access to carcass parameters
O.ACCESS_TECHNICIANS	FDP_ACC.1(1) FDP_ACF.1-NIAP-0407(1) FIA_UAU.2 FIA_UID.2 FMT_MSA.1(1) FMT_MSA.3(1) FMT_MTD.1(1)	**FDP_ACC.1(1) and FDP_ACF.1-NIAP-0407(1)** - These SFRs address the objective by specifying that Technicians have view and delete access to images, carcass parameters, and records. **FIA_UAU.2 and FIA_UID.2** – These SFRs address the objective by specifying that the TOE provide I&A functions. **FMT_MSA.1(1)** - This SFR addresses the objective by specifying that Technicians have control over the login credentials for Operators, PlantIT, and Technicians. **FMT_MSA.3(1)** – This SFR addresses this objective by allowing Technicians to change the initial security attributes (role) for users. **FMT_MTD.1(1)** - This SFR addresses the objective by specifying that Technicians have control over the camera parameters, communication parameters, and security banner.
O.ACCESS_VENDORS	FDP_ACC.1(1) FDP_ACF.1-NIAP-0407(1) FIA_UAU.2 FIA_UID.2 FMT_MOF.1 FMT_MSA.1(2) FMT_MSA.3(1) FMT_MTD.1(2)	**FDP_ACC.1(1) and FDP_ACF.1-NIAP-0407(1)** - These SFRs address the objective by specifying that Vendors have view and delete access to images, carcass parameters, and records. **FIA_UAU.2 and FIA_UID.2** – These SFRs address the objective by specifying that the TOE provide I&A functions. **FMT_MOF.1** - This SFR addresses the objective by specifying that Vendors have the ability to upgrade the TOE software. **FMT_MSA.1(2)** - This SFR addresses the objective by specifying that Vendors have control over the login credentials for Graders and Vendors. **FMT_MSA.3(1)** – This SFR addresses this objective by allowing Vendors to change the initial security attributes (role) for users. **FMT_MTD.1(2)** - This SFR addresses the objective by specifying that Vendors have control over the inactivity timers.

Objective	Addressed By	Rationale
O.AUDIT_GENERATION	FAU_GEN.1-NIAP-0407(1) FAU_GEN.2-NIAP-0407(1)	**FAU_GEN.1-NIAP-0407(1) and FAU_GEN.2-NIAP-0407(1) -** These SFRs address the objective by specifying that audits for specific events be generated and that the data include the relevant userid when applicable.
O.DATA_DELIVERY	FDP_ACC.1(1) FDP_ACF.1-NIAP-0407(1)	**FDP_ACC.1(1) and FDP_ACF.1-NIAP-0407(1)** - These SFRs address the objective by specifying that Graders are able to transfer images and records.
O.DATA_PROTECTION	FDP_ACC.1(1) FDP_ACF.1-NIAP-0407(1)	**FDP_ACC.1(1) and FDP_ACF.1-NIAP-0407(1)** - These SFRs address the objective by specifying that no roles are able to modify images and records, and that Technicians and Vendors may not delete images or records until they have been transferred.
O.DATA_STORAGE	FDP_ACC.1(1) FDP_ACF.1-NIAP-0407(1)	**FDP_ACC.1(1) and FDP_ACF.1-NIAP-0407(1)** - These SFRs address the objective by specifying that no roles nor the TOE may delete images or records until they have been transferred.
O.DISPLAY_BANNER	FTA_TAB.1	**FTA_TAB.1** - This SFR addresses the objective by specifying that an access banner be displayed for all interactive sessions.
O.INACTIVITY	FTA_SSL.3	**FTA_SSL.3** - This SFR addresses the objective by specifying that interactive sessions be terminated after a period of inactivity.
O.MANAGE	FMT_SMF.1(1) FMT_SMR.1(1)	**FMT_SMF.1(1)** - This SFR addresses the objective by specifying the management functions provided by the TOE. **FMT_SMR.1(1)** - This SFR addresses the objective by specifying the roles supported by the TOE.
O.MEDIATE	FDP_ACC.1(1) FDP_ACF.1-NIAP-0407(1)	**FDP_ACC.1(1) and FDP_ACF.1-NIAP-0407(1)** - These SFRs address the objective by specifying all the permitted accesses to user data by the defined roles.
O.SELFTEST	FPT_TST_EXT.1	**FPT_TST_EXT.1** - This SFR addresses the objective by specifying that the TOE perform tests to verify the integrity of the executable code and appropriate TSF data.
O.TOE_ACCESS	FDP_ACC.1(1) FDP_ACF.1-NIAP-0407(1) FIA_AFL.1 FIA_ATD.1 FIA_SOS.1 FIA_UAU.2 FIA_UID.2 FIA_USB.1 FMT_MOF.1 FMT_MSA.1(1) FMT_MSA.1(2)	**FDP_ACC.1(1) and FDP_ACF.1-NIAP-0407(1)** - These SFRs address the objective by specifying all the permitted accesses to user data by the defined roles. The SFRs related to I&A address the objective by specifying that successfully complete the I&A process before gaining access to the TOE (**FIA_UID.2** and **FIA_UAU.2**). The mechanism has a defined strength (**FIA_SOS.1**) defined in part by the handling of consecutive login failures (**FIA_AFL.1**). Upon successful login, security attributes associated with the user (**FIA_ATD.1**) are bound to the user session (**FIA_USB.1**)so that appropriate management functions

Objective	Addressed By	Rationale
	FMT_MSA.3(1) FMT_MTD.1(1) FMT_MTD.1(2) FMT_SMF.1(1) FMT_SMR.1(1)	may be provided. The SFRs related to management define the management functions (**FMT_SMF.1**) provided to the various roles (**FMT_SMR.1**). The specific management access available to each role is defined for management functions (**FMT_MOF.1**), security attribute handling (**FMT_MSA.1** and **FMT_MSA.3**) and TSF data (**FMT_MTD.1**).

6.5 IT Environment security functional requirements rationale

6.5.1 Mapping of IT Environment Objectives to SFRs

The following table presents a mapping of the objectives to the SFRs levied on the IT Environment in this PP.

Table 6.8 – Mapping of IT Environment Objectives to SFRs/SARs

	OE.ACCESS_REVIEWERS	OE.ACCESS_SYSADMINS	OE.AUDIT_BACKUP	OE.AUDIT_GENERATION	OE.AUDIT_REVIEW	OE.AUDIT_STORAGE	OE.DATA_PROTECTION	OE.DEDICATED_SYSTEMS	OE.DISPLAY_BANNER	OE.I&A	OE.INACTIVITY	OE.NETWORK_ACCESS	OE.NOEVIL	OE.PHYSICAL_ACCESS	OE.RESIDUAL_INFORMATION	OE.SECURE_COMMS	OE.SELFTEST	OE.TIME_STAMPS	OE.TOE_ACCESS	OE.TRUST_IT
FAU_GEN.1-NIAP-0407(2)				X																
FAU_GEN.2-NIAP-0410(2)				X																
FAU_SAR.1					X															
FAU_SAR.2					X															
FAU_STG.1						X														
FDP_ACC.1(2)	X						X												X	
FDP_ACF.1-NIAP-0407(2)	X						X												X	
FDP_IFC.1												X								
FDP_IFF.1-NIAP-0407												X								

	OE.ACCESS_REVIEWERS	OE.ACCESS_SYSADMINS	OE.AUDIT_BACKUP	OE.AUDIT_GENERATION	OE.AUDIT_REVIEW	OE.AUDIT_STORAGE	OE.DATA_PROTECTION	OE.DEDICATED_SYSTEMS	OE.DISPLAY_BANNER	OE.I&A	OE.INACTIVITY	OE.NETWORK_ACCESS	OE.NOEVIL	OE.PHYSICAL_ACCESS	OE.RESIDUAL_INFORMATION	OE.SECURE_COMMS	OE.SELFTEST	OE.TIME_STAMPS	OE.TOE_ACCESS	OE.TRUST_IT
FDP_RIP.1															X					
FIA_UAU.1										X										
FIA_UID.1										X										
FMT_MSA.1(3)		X																	X	
FMT_MSA.3(2)		X																	X	
FMT_MTD.1(3)		X																	X	
FMT_SMF.1(2)																			X	
FMT_SMR.1(2)																			X	
FPT_AMT.1																	X			
FPT_STM.1																		X		
FTA_SSL.3(2)											X									
FTA_TAB.1(2)									X											
FTP_ITC.1																X				
ADV_OPE.1			X					X					X	X						X
ADV_PRE.1			X					X					X	X						X

6.5.2 Rationale for IT Environment Objectives

Table 6.9 – IT Environment Security Objectives to SFRs/SARs Rationale

Objective	Addressed By	Rationale
OE.ACCESS_REVIEWERS	FDP_ACC FDP_ACF.1-NIAP-0407(2)	**FDP_ACC and FDP_ACF.1-NIAP-0407(2) 1** - These SFRs address the objective by specifying that Reviewers have view access to captured images.
OE.ACCESS_SYSADMINS	FMT_MSA.1(3) FMT_MSA.3(2) FMT_MTD.1(3)	**FMT_MSA.1(3)** – This SFR addresses the objective by specifying that SysAdmins configure the access credentials for operating

Objective	Addressed By	Rationale
		system logins. **FMT_MSA.3(2) -** This SFR addresses this objective by allowing SysAdmins to change the initial security attributes (role) for users. **FMT_MTD.1(3)** – This SFR addresses the objective by specifying that SysAdmins configure the network access parameters, time, inactivity timer for sessions controlled by the OS, and security banner for logins controlled by the OS.
OE.AUDIT_BACKUP	ADV_OPE.1 ADV_PRE.1	**ADV_OPE.1 and ADV_PRE.1** - These SARs address the objective since installation and operational requirements on the administrator are addressed in these documents.
OE.AUDIT_GENERATION	FAU_GEN.1-NIAP-0407(2) FAU_GEN.2-NIAP-0407(2)	**FAU_GEN.1-NIAP-0407(2) and FAU_GEN.2-NIAP-0407(2) -** These SFRs address the objective by specifying that audits for specific events be generated and that the data include the relevant userid when applicable.
OE.AUDIT_REVIEW	FAU_SAR.1 FAU_SAR.2	**FAU_SAR.1 and FAU_SAR.2** - These SFRs address the objective by specifying that authorized users be able to review the audit logs.
OE.AUDIT_STORAGE	FAU_STG.1	**FAU_STG.1** – This SFR addresses the objective by specifying that the audit records be protected from unauthorized modification or deletion.
OE.DATA_PROTECTION	FDP_ACC FDP_ACF.1-NIAP-0407(2)	**FDP_ACC and FDP_ACF.1-NIAP-0407(2) -** These SFRs address the objective by specifying that no IT Env. roles have modify or delete access to the images or records.
OE.DEDICATED_SYSTEMS	ADV_OPE.1 ADV_PRE.1	**ADV_OPE.1 and ADV_PRE.1 -** These SARs address the objective since installation and operational requirements on the IT systems are addressed in these documents.
OE.DISPLAY_BANNER	FTA_TAB.1(2)	**FTA_TAB.1(2) -** This SFR addresses the objective by specifying that the IT Env. Display a banner to interactive sessions.
OE.I&A	FIA_UAU.1 FIA_UID.1	**FIA_UAU.1 and FIA_UID.1-** These SFRs address the objective by specifying that the IT Env. perform an I&A function.
OE.INACTIVITY	FTA_SSL.3(2)	**FTA_SSL.3(2)** - This SFR addresses the objective by specifying that inactive interactive sessions be terminated.
OE.NETWORK_ACCESS	FDP_IFC FDP_IFF.1-NIAP-0407	**FDP_IFC and FDP_IFF.1-NIAP-0407-** These SFRs address the objective by specifying that only specifically authorized IT Env. systems are able to send traffic to or receive traffic from the

Objective	Addressed By	Rationale
		systems hosting the TOE.
OE.NO_EVIL	ADV_OPE.1 ADV_PRE.1	**ADV_OPE.1 and ADV_PRE.1 -** These SARs address the objective since requirements on the administrator are addressed in these documents.
OE.PHYSICAL_ACCESS	ADV_OPE.1 ADV_PRE.1	**ADV_OPE.1 and ADV_PRE.1 -** These SARs address the objective since installation and operational requirements on physical access are addressed in these documents.
OE.RESIDUAL_INFORMATION	FDP_RIP.1	**FDP_RIP.1-** This SFR addresses the objective by specifying that the memory (at a minimum) be cleared before it is reallocated to another process.
OE.SECURE_COMMS	FTP_ITC.1	**FTP_ITC.1-** This SFR addresses the objective by specifying that a trusted channel be used to protect sensitive information from disclosure or modification.
OE.SELFTEST	FPT_AMT.1	**FPT_AMT.1-** This SFR addresses the objective by specifying that self tests be performed, at a minimum on start-up, for any mechanism upon which the TOE relies.
OE.TIME_STAMPS	FPT_STM.1	**FPT_STM.1**- This SFR addresses the objective by specifying that the IT Env. be able to provide time stamps.
OE.TOE_ACCESS	FDP_ACC FDP_ACF.1-NIAP-0407(2) FMT_MSA.1(2) FMT_MSA.3(2) FMT_MTD.1(3) FMT_SMF.1(2) FMT_SMR.1(2)	**FDP_ACC and FDP_ACF.1-NIAP-0407(2) -** These SFRs address the objective by specifying the access privileges for user data for all roles. The SFRs related to management define the management functions (**FMT_SMF.1**) provided to the various roles (**FMT_SMR.1**). The specific management access available to each role is defined for security attribute handling (**FMT_MSA.1** and **FMT_MSA.3**) and TSF data (**FMT_MTD.1**).
OE.TRUST_IT	ADV_OPE.1 ADV_PRE.1	**ADV_OPE.1 and ADV_PRE.1 -** These SARs address the objective since requirements on the administrator are addressed in these documents.

6.6 TOE security assurance requirements rationale

6.6.1 Mapping of Development Objectives to SARs

The following table presents a mapping of the objectives to the SARs levied on the TOE in this PP.

Table 6.10 – Mapping of Development Objectives to SARs

	ADV_ARC.1	ADV_FSP.2	ADV_TDS.1	AGD_OPE.1	AGD_PRE.1	ALC_CMC.2	ALC_CMS.2	ALC_DEL.1	ALC_FLR.2	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_VAN.2
OD.ADMIN_GUIDANCE				X	X								
OD.CONFIGURATION_IDENTIFICATION						X	X						
OD.DELIVERY_INTEGRITY								X					
OD.DEVELOPMENT_INTEGRITY						X	X						
OD.DOCUMENTED_DESIGN	X	X	X										
OD.FLAW_REMEDIATION									X				
OD.PARTIAL_SELF_PROTECTION	X												
OD.TEST										X	X	X	
OD.VULNERABILITY_ANALYSIS													X

6.6.2 Rationale for Development Objectives

Table 6.11 – Development Security Objectives to SARs Rationale

Objective	Addressed By	Rationale
OD.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management.	**AGD_OPE.1** **AGD_PRE.1**	**AGD_OPE.1** - The operational user guidance provides a measure of confidence that non-malicious users, administrators, application providers and others exercising the external interfaces of the TOE will understand the secure operation of the TOE and will use it as intended. **AGD_PRE.1** - Preparative procedures are useful for ensuring that the TOE has been received and installed in a secure manner as intended by the developer. The requirements for preparation call for a secure transition from the delivered TOE to its initial operational environment.
OD.CONFIGURATION_IDENTIFICATION The configuration of the TOE is	**ALC_CMC.2** **ALC_CMS.2**	**ALC_CMC.2** - A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labeling the TOE with its

Objective	Addressed By	Rationale
fully identified in a manner that will allow known implementation errors to be correlated with operational systems.		reference ensures that users of the TOE can be aware of which instance of the TOE they are using. **ALC_CMS.2** - Placing the TOE itself, the parts that comprise the TOE, and the evaluation evidence required by the other SARs under CM provides assurance that they have been modified in a controlled manner with proper authorizations.
OD.DELIVERY_INTEGRITY The development environment shall ensure that the TOE is delivered to the consumer without compromising the integrity of the TOE.	**ALC_DEL.1**	**ALC_DEL.1** - The requirements for delivery call for system control and distribution facilities and procedures that detail the measures necessary to provide assurance that the security of the TOE is maintained during distribution of the TOE to the user.
OD.DEVELOPMENT_INTEGRITY The development environment shall ensure that the integrity of the source code of the TOE is protected.	**ALC_CMC.2** **ALC_CMS.2**	**ALC_CMC.2** - A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labeling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using. **ALC_CMS.2** - Placing the TOE itself, the parts that comprise the TOE, and the evaluation evidence required by the other SARs under CM provides assurance that they have been modified in a controlled manner with proper authorizations.
OD.DOCUMENTED_DESIGN The design of the TOE is adequately and accurately documented.	**ADV_ARC.1** **ADV_FSP.2** **ADV_TDS.1**	**ADV_ARC.1** - The objective of this family is for the developer to provide a description of the security architecture of the TSF. This will allow analysis of the information that, when coupled with the other evidence presented for the TSF, will confirm the TSF achieves the desired properties. **ADV_FSP.2** - This family levies requirements upon the functional specification, which describes the TSF interfaces (TSFIs). The TSFIs consist of all means for users to invoke a service from the TSF (by supplying data that is processed by the TSF) and the corresponding responses to those service invocations. It provides the purpose, method of use, parameters, and parameter descriptions for all TSFIs. **ADV_TDS.1** - The design description of a TOE provides both context for a description of the TSF, and a thorough description of the TSF.
OD.FLAW_REMEDIATION Procedures to address security issues in the TOE will be documented and followed.	**ALC_FLR.2**	**ALC_FLR.2** - Flaw remediation requires that discovered security flaws be tracked and corrected by the developer.
OD.PARTIAL_SELF_PROTE	**ADV_ACR.1**	**ADV_ARC.1** – The architecture document describes how the TOE protects itself from external interference

Objective	Addressed By	Rationale
CTION The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.		and tampering, and prevents bypass of the security mechanisms.
OD.TEST The TOE will undergo testing by the developer and an independent party to detect obvious errors in the implementation.	**ATE_COV.1** **ATE_FUN.1** **ATE_IND.2**	**ATE_COV.1** - This family establishes that the TSF has been tested against its functional specification. **ATE_FUN.1** - Functional testing performed by the developer provides assurance that the tests in the test documentation are performed and documented correctly. This family contributes to providing assurance that the likelihood of undiscovered flaws is relatively small. **ATE_IND.2** - The objectives of this family are verifying the developer testing and performing additional tests by the evaluator, in order to demonstrate that the TOE operates in accordance with its design representations and guidance documents.
OD.VULNERABILITY_ANALYSIS The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	**AVA_VAN.2**	**AVA_VAN.2** - A vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities. The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the evaluator assuming an attack potential of Basic.

6.7 TOE Security Functional Requirement Dependency Analysis

The following table presents an analysis of the dependencies of the SFRs levied against the TOE.

Table 6.12 – TOE SFR Dependency Analysis

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1-NIAP-0407	No other components.	FPT_STM.1	Satisfied by the IT Environment
FAU_GEN.2-NIAP-0410	No other components.	FAU_GEN.1, FIA_UID.1	Satisfied by FAU_GEN.1-NIAP-0407(1) Satisfied by FIA_UID.2
FDP_ACC.1	No other components.	FDP_ACF.1	Satisfied by FDP_ACF.1-NIAP-0407(1)
FDP_ACF.1-NIAP-0407	No other components.	FDP_ACC.1, FMT_MSA.3	Satisfied by FDP_ACC.1(1) Satisfied by FMT_MSA.3(1)

SFR	Hierarchical To	Dependency	Rationale
FIA_AFL.1	No other components.	FIA_UAU.1	Satisfied by FIA_UAU.2
FIA_ATD.1	No other components.	None	n/a
FIA_SOS.1	No other components.	None	n/a
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UID.2	FIA_UID.1	None	n/a
FIA_USB.1	No other components.	FIA_ATD.1	Satisfied
FMT_MOF.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied by FMT_SMF.1(1) Satisfied by FMT_SMR.1(1)
FMT_MSA.1	No other components.	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1 FMT_SMR.1	Satisfied by FDP_ACC.1(1) Satisfied by FMT_SMF.1(1) Satisfied by FMT_SMR.1(1)
FMT_MSA.3	No other components.	FMT_MSA.1, FMT_SMR.1	Satisfied by FMT_MSA.1(1 and 2) Satisfied by FMT_SMR.1(1)
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied by FMT_SMF.1(1) Satisfied by FMT_SMR.1(1)
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by FIA_UID.2
FPT_TST_EXT.1	No other components.	FPT_AMT.1	Satisfied by the IT Environment
FTA_SSL.3	No other components.	None	n/a

6.8 IT Environment Security Functional Requirement Dependency Analysis

The following table presents an analysis of the dependencies of the SFRs levied against the IT Environment.

Table 6.13 – IT Environment SFR Dependency Analysis

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1-NIAP-0407	No other components.	FPT_STM.1	Satisfied
FAU_GEN.2-NIAP-0410	No other components.	FAU_GEN.1, FIA_UID.1	Satisfied by FAU_GEN.1-NIAP-0407(1) Satisfied
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied by FAU_GEN.1-NIAP-0407(1)
FAU_SAR.2	No other components.	FAU_SAR.1	Satisfied
FAU_STG.1	No other components.	FAU_GEN.1	Satisfied by FAU_GEN.1-NIAP-0407(1)
FDP_ACC.1	No other components.	FDP_ACF.1	Satisfied by FDP_ACF.1-NIAP-0407(2)
FDP_ACF.1-NIAP-0407	No other components.	FDP_ACC.1, FMT_MSA.3	Satisfied by FDP_ACC.1(2) Satisfied by FMT_MSA.3(2)

SFR	Hierarchical To	Dependency	Rationale
FDP_IFC.1	No other components.	FDP_IFF.1	Satisfied by FDP_IFF.1-NIAP-0407
FDP_IFF.1-NIAP-0407	No other components.	FDP_IFC.1, FMT_MSA.3	Satisfied by FDP_IFC.1 Satisfied by FMT_MSA.3(2)
FDP_RIP.1	No other components.	None	n/a
FIA_UAU.1	No other components.	FIA_UID.1	Satisfied
FIA_UID.1	No other components.	None	n/a
FIA_USB.1	No other components.	FIA_ATD.1	Satisfied
FMT_MSA.1	No other components.	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1 FMT_SMR.1	Satisfied by FDP_ACC.1(2) Satisfied Satisfied by FMT_SMF.1(2) Satisfied by FMT_SMR.1(2)
FMT_MSA.3	No other components.	FMT_MSA.1, FMT_SMR.1	Satisfied by FMT_MSA.1(3) Satisfied by FMT_SMR.1(2)
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied by FMT_SMF.1(2) Satisfied by FMT_SMR.1(2)
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied
FPT_AMT.1	No other components.	None	n/a
FPT_STM.1	No other components.	None	n/a
FTA_SSL.3	No other components.	None	n/a
FTA_TAB.1	No other components.	None	n/a
FTP_ITC.1	No other components.	None	n/a

7 Acronyms

Table 7.1 – List of Acronyms

BR CIM	Basic Robustness Consistency Instruction Manual
CC	Common Criteria
CFR	Code of Federal Regulations
CM	Configuration Management
DoD	Department of Defense
EAL	Evaluation Assurance Level
FOUO	For Official Use Only
I&A	Identification and Authentication
IA	Information Assurance
ID	Identification
IGS	Instrument Grading System
IP	Internet Protocol
IT	Information Technology
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
NIAP	National Information Assurance Partnership
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SBU	Sensitive But Unclassified
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TCP	Transmission Control Protocol
TIFF	Tagged Image File Format
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
USDA	United States Department of Agriculture