National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

U. S. Government Protection Profile
USDA INSTRUMENT GRADING SYSTEMS
FOR
BASIC ROBUSTNESS ENVIRONMENTS,
Version 1.0

Report Number: CCEVS-VR-VID10315-2008
Dated: 23 September 2008
Version 1.0

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validator

Deborah Downs

Common Criteria Testing Laboratory

Evaluation Team
COACT, Inc
Rivers Ninety Five
9140 Guilford Road, Suite G
Columbia, MD 21046-2587

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the US Government Protection Profile for United States Department of Agriculture (USDA) Instrument Grading Systems for Basic Robustness Environments, version 1.0. It presents the evaluation results, their justifications, and the conformance result.

The evaluation of the US Government Protection Profile for USDA Instrument Grading Systems for Basic Robustness Environments, Version 1.0, was performed by COACT, Inc., CAFÉ Lab CCTL in the United States and was completed on 22 September 2008. The Protection Profile (PP) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 3.1) for conformance to the APE requirements of the Common Criteria for IT Security Evaluation (Version 3.1).

This Validation Report applies only to the specific version of the PP as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. The information contained in this Validation Report is not an endorsement of the US Government Protection Profile for USDA Instrument Grading Systems for Basic Robustness Environments, Version 1.0, dated September 16, 2008 by any agency of the U.S. Government and no warranty of the PP is either expressed or implied.

The COACT, Inc., CAFÉ Lab evaluation team concluded that the Common Criteria requirements for a PP Evaluation have been met.

The technical information included in this report was obtained from the US Government Protection Profile for USDA Instrument Grading Systems for Basic Robustness Environments, Version 1.0, dated September 16, 2008 and the Evaluation Technical Report for US Government Protection Profile for USDA Instrument Grading Systems for Basic Robustness Environments, dated September 23, 2008, Document No. F2-0908-001 produced by COACT, Inc., CAFÉ Lab.

2. IDENTIFICATION and OVERVIEW

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The CCEVS assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List.

2.1 Identification

The following information completely identifies the Protection Profile:

Evaluation Identifiers for USDA Instrument Grading Systems for Basic Robustness Environments, Version 1.0	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluation Technical Report	US Government Protection Profile for USDA Instrument Grading Systems for Basic Robustness Environments Evaluation Technical Report, dated September 23, 2008, Document No. F2-0908-001
Conformance Result	Part 2 extended, Part 3 conformant
Version of CC	CC Version 3.1 and all applicable NIAP CCEVS and International Interpretations effective on May 1, 2008
Version of CEM	CEM Version 3.1 and all applicable NIAP CCEVS and International Interpretations effective on May 1, 2008
Sponsor	**USDA**
Developer	**COACT, Inc. and CCC Consulting**
Evaluator(s)	**COACT, Inc.** Brian Pleffner Greg Beaver Robert Roland
Validator(s)	**NIAP CCEVS** Deborah Downs

2.2 PP 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.

2.2.1 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 2.1.

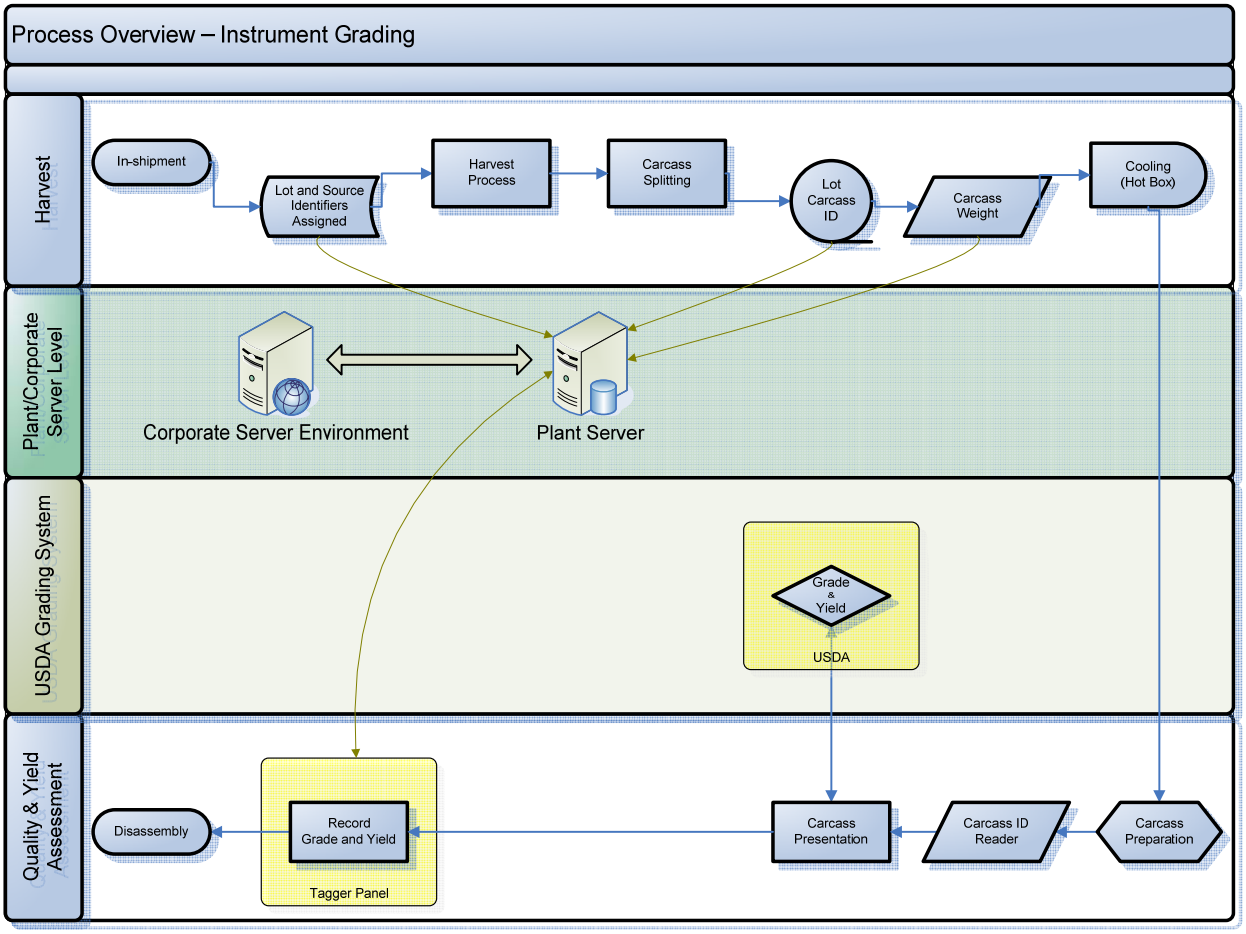

Figure 2.1 - Historical USDA Grading Process

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 2.2 illustrates the process utilizing this approach.

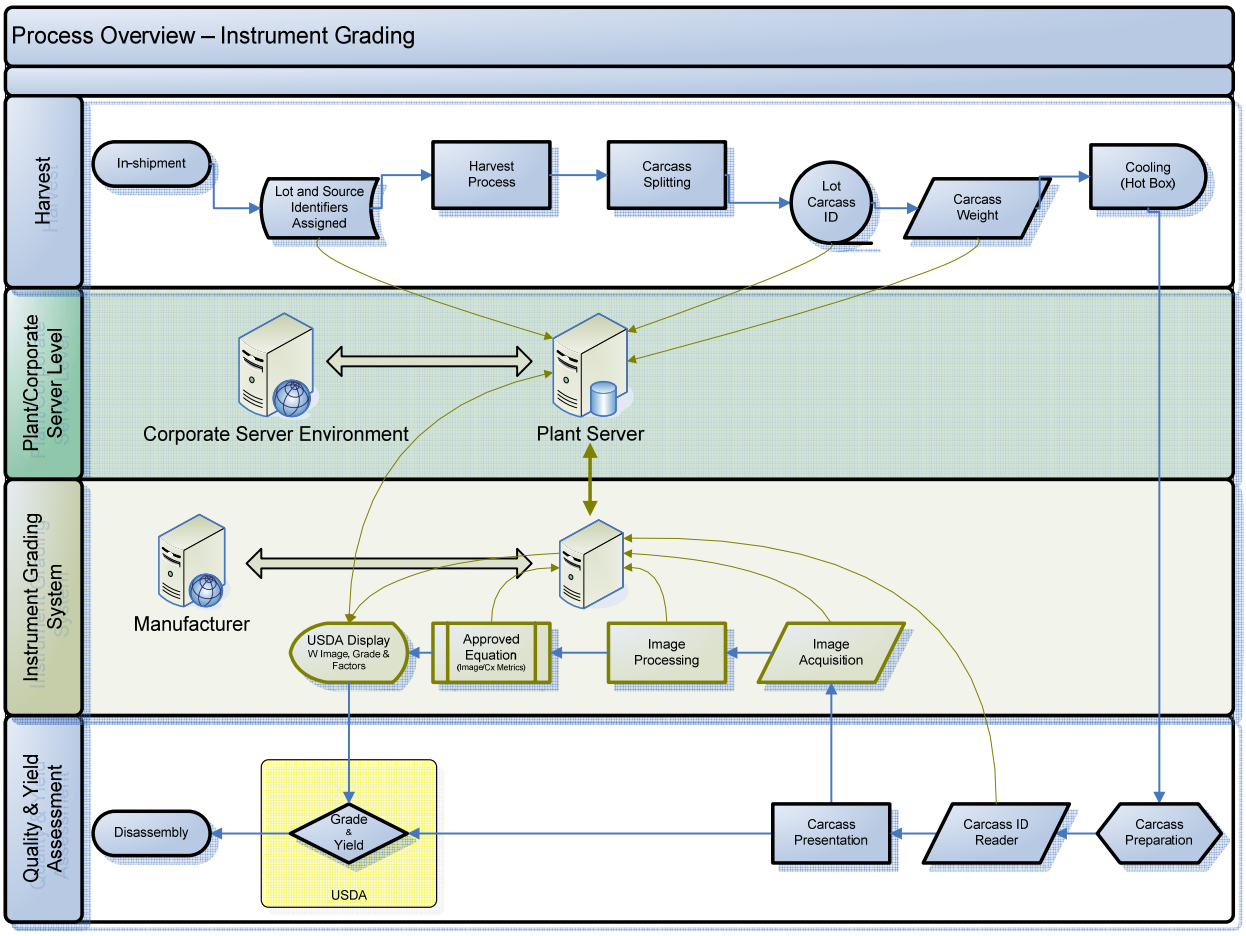

Figure 2.2 – USDA Grading Process Using Prediction Equation

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 2.2 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 2.3 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.

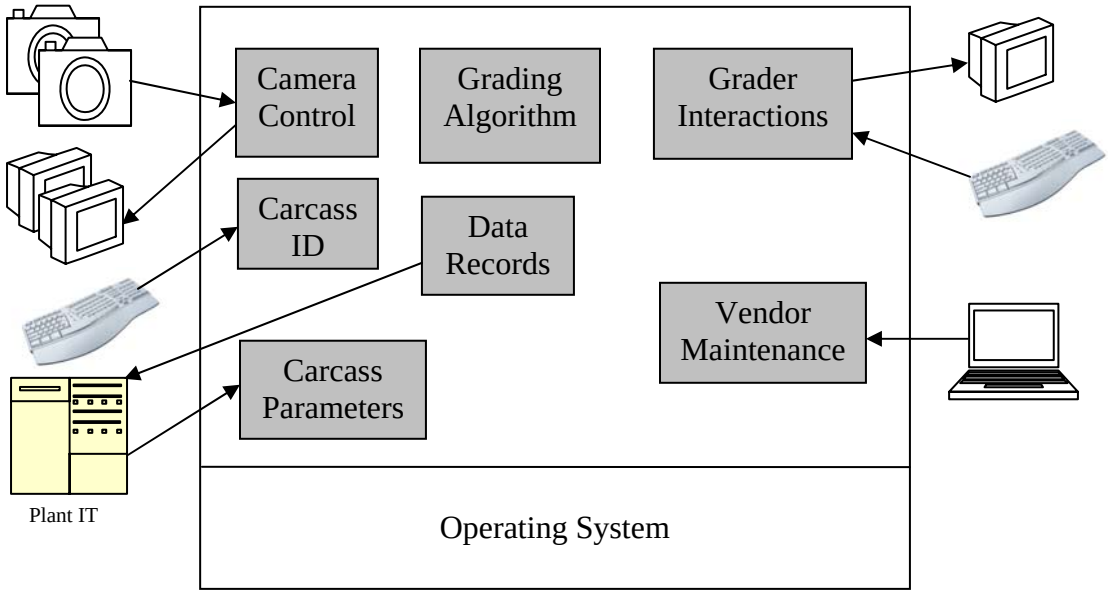

Figure 2.3 – Representative TOE Implementation

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.

2.3 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.

2.3.1 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.

3 THREATS, POLICIES, and ASSUMPTIONS

3.1 Threats to Security

The Protection Profile identified the following Threats:

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.

Threat	Description of Threat
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.
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.

3.2 Operational Security Policies

The Operational Security Policies defined for the TOE are as follows:

Policy	Policy Description
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.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ADMIN_ACCESS	Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.
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.
P.I_AND_A	All users must be identified and authenticated prior to accessing any controlled resources with the exception of public objects.
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.

P.SYSTEM_INTEGRITY	The TOE shall provide the ability to periodically validate its correct operation.
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.

3.3 Assumptions

The specific conditions below are assumed to exist in a PP-compliant TOE environment.

Assumption	Assumption Description
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 ARCHITECTURAL INFORMATION

Figure 3.1 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:

- The number of cameras used to capture images of the carcasses. Each camera may be connected to a separate system.
- Processing or storage requirements for the system. A single system may not have adequate resources to perform all of the TOE functions.
- 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 3.1 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.

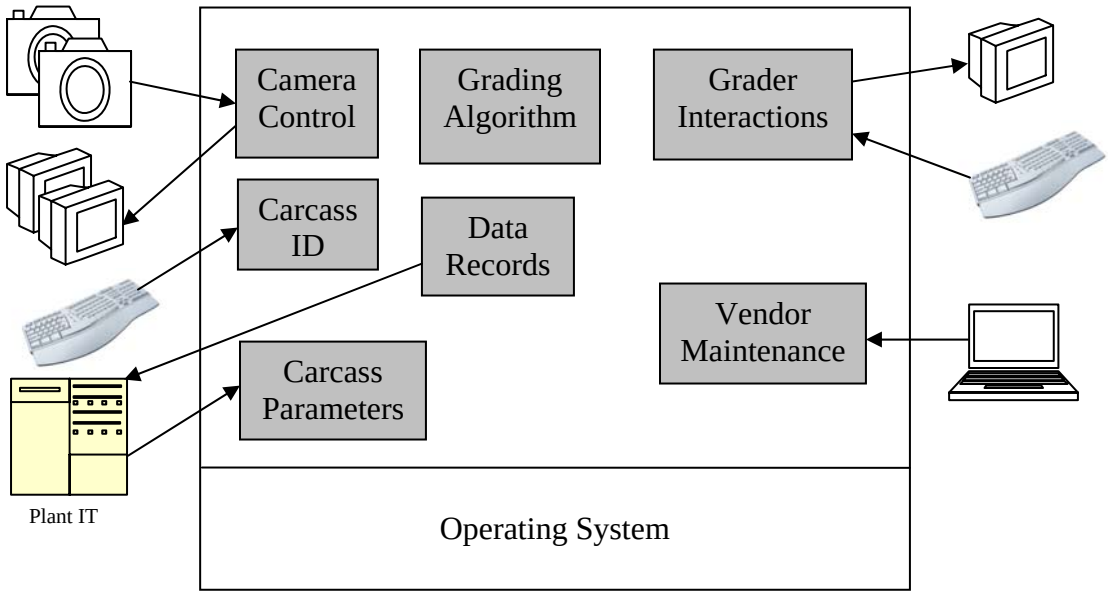

Figure 3.1 – Representative TOE Implementation

5 DOCUMENTATION

US Government Protection Profile for USDA Instrument Grading Systems for Basic Robustness Environments, Version 1.0.

6 RESULTS OF THE EVALUATION

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted in accordance with the APE sections in the Common Criteria, Version 3.1; CEM, Version 3.1, and all applicable NIAP CCEVS and International Interpretations in effect on May 1, 2008.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of the APE assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Comments or Work Pack Assessment Tables for an evaluation activity that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. No constraints or assumptions were identified in performing this evaluation.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

Chapter 4, Evaluation Results, in the Evaluation Team's ETR, states: "The US Government Protection Profile for USDA Instrument Grading Systems for Basic Robustness Environments was successfully evaluated."

Chapter 5, Conclusions, in the Evaluation Team's ETR, states: "The US Government Protection Profile for USDA Instrument Grading Systems for Basic Robustness Environments has satisfied the requirements of the APE Assurance Requirements. The PP was assessed against the requirements as stated in the Common Methodology for Information Technology Security Evaluation Part 2, Version 3.1."

7 VALIDATION COMMENTS/RECOMMENDATIONS

None

8 ACRONYMS

CC	Common Criteria
EAL	Evaluation Assurance Level
I&A	Identification and Authentication
ID	Identification
IGS	Instrument Grading System
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PP	Protection Profile
TCP	Transmission Control Protocol

9 BIBLIOGRAPHY

The Validation Team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluatio*n, version 3.1, September 2006, Part 1
- *Common Criteria for Information Technology Security Evaluatio*n, version 3.1, September 2006, Part 2
- *Common Criteria for Information Technology Security Evaluatio*n, version 3.1, September 2006, Part 3
- *Common Evaluation Methodology for Information Technology Security Evaluation* – Evaluation Methodology, version 3.1, September 2006.
- US Government Protection Profile for USDA Instrument Grading Systems for Basic Robustness Environments, Version 1.0, dated September 16, 2008
- Evaluation Technical Report for US Government Protection Profile for USDA Instrument Grading Systems for Basic Robustness Environments dated September 23, 2008, Document No. F2-0908-001
- [7CFR54.2] Code of Federal Regulations, Title 7, Volume 3, PART 54, Section 54.2, Revised as of January 1, 2002.