

DHS/ST/TSL-19/30

Management Plan for the Certification Test and Evaluation of Checkpoint Property Screening Systems (CPSS)

William Petracci, Test Director, Independent Test and
Evaluation

U.S. Department of Homeland Security
Science and Technology Directorate
William J. Hughes Technical Center
Atlantic City International Airport, NJ 08405

May 8, 2019

Final

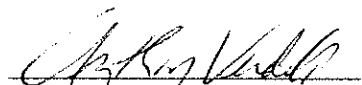


U.S. Department of Homeland Security
Science and Technology Directorate

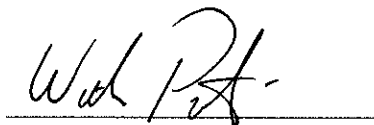
NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Homeland Security in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof. The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

This management plan (DHS/ST/TSL-19/30) has been reviewed and is approved for publication and use subject to the constraints of the distribution statement.



Anthony Vendetti
Test Lead, Checkpoint Property Screening System Program
Office of Independent Test & Evaluation
Transportation Security Laboratory
Science & Technology Directorate



William Petracci
Test Director
Office of Independent Test & Evaluation
Transportation Security Laboratory
Science & Technology Directorate

Kenneth (Andy) Lee
Operational Test Agent
Director, Test & Evaluation Division
Acquisition Program Management
Transportation Security Administration

Technical Report Documentation Page

1. Report No. DHS/ST/TSL-19/30		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle Management Plan for the Certification Test and Evaluation of Checkpoint Property Screening Systems (CPSS)				5. Report Date May 8, 2019	
				6. Performing Organization Code	
7. Author(s) William Petracci, Test Director, Independent Test and Evaluation				8. Performing Organization Report No. DHS/ST/TSL-19/30	
9. Performing Organization Name and Address U.S. Department of Homeland Security Science and Technology Directorate Transportation Security Laboratory, TSL-1 William J. Hughes Technical Center Atlantic City International Airport, NJ 08405				10. Work Unit No. (TRAIS)	
				11. Contract or Grant No.	
12. Sponsoring Agency Name and Address U.S. Department of Homeland Security Science and Technology Directorate Transportation Security Laboratory, TSL-1 William J. Hughes Technical Center Atlantic City International Airport, NJ 08405				13. Type of Report and Period Covered Program Management Plan - Final	
				14. Sponsoring Agency Code ST	
15. Supplementary Notes					
16. Abstract This document, the Management Plan for the Certification Test and Evaluation of Checkpoint Property Screening Systems (CPSS), defines the process by which the Independent Test & Evaluation (IT&E) Division of the Transportation Security Laboratory (TSL) determines if candidate explosive detection systems satisfy the criteria specified by the TSA in the <i>TSA Accessible Property Screening System (APSS) Detection Requirements</i> [5]. This document also provides guidance to vendors producing candidate systems of the data and documentation required by and the nominal timeline for the certification testing process.					
17. Key Words Accessible Property Screening Systems Checkpoint Property Screening Systems Management Plan Functional Requirements Document Certification Testing and Evaluation Checkpoint Configuration Management Certification Data Package			18. Distribution Statement		
19. Security Classif. (of this report) Unclassified		20. Security Classif. (of this page) Unclassified		21. No. of Pages 23	
				22. Price	

Reproduction of completed page authorized

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	iv
ACRONYMS	v
1. Certification Test & Evaluation Process Overview	1
1.1 Purpose	1
1.2 CT&E Activities	1
1.2.1 Certification Readiness Testing	3
1.2.2 Vendor Request for Certification Testing	3
1.2.3 Evaluation of Vendor Certification Data Package	3
1.2.4 CPSS Installation and Integration (I&I)	4
1.2.5 Emulator Installation and Acceptance	4
1.2.6 Emulator and System Training	5
1.2.7 Configuration Management (CM)	5
1.2.8 Pre-Certification Test and Evaluation	5
1.2.9 Certification Testing	5
1.2.10 Reporting of Results and Certification Recommendation	6
1.2.11 Certification Process Schedule	7
1.3 Organizational Roles and Responsibilities	7
1.3.1 TSA office of APM	7
1.3.2 IT&E Test Director (TSL)	7
1.3.3 Alternative Government-Approved Test Facility Lead	8
2. Vendor Instructions and Certification Data Package (CDP) Requirements	8
2.1 Purpose	8
2.2 Identification of Systems and Emulator	8
2.3 Theory of Operation	9
2.4 Safety	9
2.5 Data Requirements	9
2.5.1 Data Requirements for Candidate CPSS Not Previously Accepted for Certification Testing	9
2.5.2 Data Management Procedures	13
2.5.3 Test and Evaluation Data	13
2.5.4 Simulants/Explosives Validation Data	14
2.5.5 T&E Report	14
2.5.6 Data Requirements for Candidate CPSS Previously Accepted for Certification Testing	14
3. Reference Documents	15

LIST OF FIGURES

Figure 1: CPSS CT&E Overview	2
------------------------------	---

LIST OF TABLES

Table 1. Product Configuration Baseline Matrix—Hardware	11
Table 2. Product Configuration Baseline—Software	12
Table 3. Delta Detection Test Results	15

EXECUTIVE SUMMARY

The mission of the Transportation Security Administration (TSA) is to prevent, deter, or render attacks ineffective against transportation systems and related infrastructure, a mission that includes improving the detection of weapons and explosives within divested accessible property at transportation security checkpoints. To support this mission, the TSA office of Requirements and Capabilities Analysis (RCA) has developed detection performance requirements for Checkpoint Property Screening Systems (CPSS).

The Independent Test & Evaluation (IT&E) Division of the Transportation Security Laboratory (TSL) has developed a Certification Test and Evaluation (CT&E) process to determine if systems meet TSA-defined CPSS explosives detection requirements. This Management Plan has been developed by IT&E and approved by the Director of the Test & Evaluation (T&E) Division, TSA office of Acquisition Program Management (APM). It outlines the framework of the CT&E process and defines the documentation and methods that will be used by IT&E for conducting CT&E. The IT&E Test Director is responsible for the contents of this Management Plan and the CPSS test plan and test procedures. The Test Director will manage or oversee the laboratory test program and provide the TSA with a test report for each CPSS tested.

ACRONYMS

APSS	Accessible Property Screening System(s)
APM	Acquisition Program Management
CDP	Certification Data Package
CFR	Code of Federal Regulations
CM	Configuration Management
CMM	Capability Maturity Model
CONOPS	Concept of Operations
CPSS	Checkpoint Property Screening System(s)
CRT	Certification Readiness Testing
CT	Computed Tomography
CT&E	Certification Test and Evaluation
DT&E	Developmental Test and Evaluation
DHS	Department of Homeland Security
DEP	Developmental Engineering Proposal
DR	Detection Rate
FA	False Alarm
FAR	False Alarm Rate
FRD	Functional Requirements Document
HME	Homemade Explosive(s)
IT&E	Independent Test and Evaluation
I&I	Installation and Integration
NRTL	Nationally Recognized Test Laboratory
QA	Quality Assurance
QLR	Quick Look Report
PCA	Physical Configuration Audit
PI	Prohibited Item
RCA	Requirements and Capabilities Analysis
S&T	Science and Technology Directorate
SSI	Sensitive Security Information
T&E	Test and Evaluation
TSA	Transportation Security Administration
TSL	Transportation Security Laboratory

1. Certification Test & Evaluation Process Overview

1.1 Purpose

The Checkpoint Property Screening System (CPSS) program has been developed by the Transportation Security Administration (TSA) to combat new and improvised threats which pose a danger to transportation systems and related infrastructure. Requirements for CPSS have been developed by the TSA office of Requirements and Capabilities Analysis (RCA) and published in *TSA Accessible Property Screening System (APSS) Detection Requirements [5]*. The Independent Test and Evaluation (IT&E) Division of the Transportation Security Laboratory (TSL), which is a part of the Science and Technology (S&T) Directorate of the Department of Homeland Security (DHS), is responsible for the Certification Test and Evaluation (CT&E) process of all checkpoint property screening systems (CPSS) submitted for certification (candidate CPSS). This plan provides an outline of the CT&E activities, organizational responsibilities, documentation, and health and safety requirements.

The purpose and objectives of the CT&E process are to:

- a. Provide an orderly progression of CT&E activities that is consistent, unbiased, and repeatable for all candidate CPSS;
- b. Evaluate the explosive detection performance of candidate CPSS against certification criteria under realistic operating conditions;
- c. Ensure appropriate configuration management (CM), quality assurance (QA) controls, and accurate documentation of evaluation results throughout the CT&E process;
- d. Provide test results for each candidate CPSS that passes certification testing to the TSA office of Acquisition Program Management (APM); and
- e. Observe and document data related to other operational considerations identified in the criteria.

1.2 CT&E Activities

Specific activities performed as part of the CT&E process are depicted in Figure 1, and include the following:

- a. Vendor submits a Certification Data Package (CDP) to the IT&E Test Director;
- b. IT&E reviews the vendor CDP;
- c. IT&E briefs the vendor on CDP evaluation results;
- d. The TSL and alternative Government-approved facility prepares for certification testing; Vendor installs and integrates (I&I) candidate CPSS and emulator at the TSL and candidate CPSS at alternative Government-approved facility;
- e. Vendor trains personnel at TSL and alternative Government-approved facility;
- f. IT&E performs pre-certification and certification testing;
- g. IT&E provides CT&E report and briefs TSA APM for CPSS that pass certification testing; and
- h. IT&E briefs the vendor of the test results.

Management Plan for the CT&E of Checkpoint Property Screening Systems (CPSS)

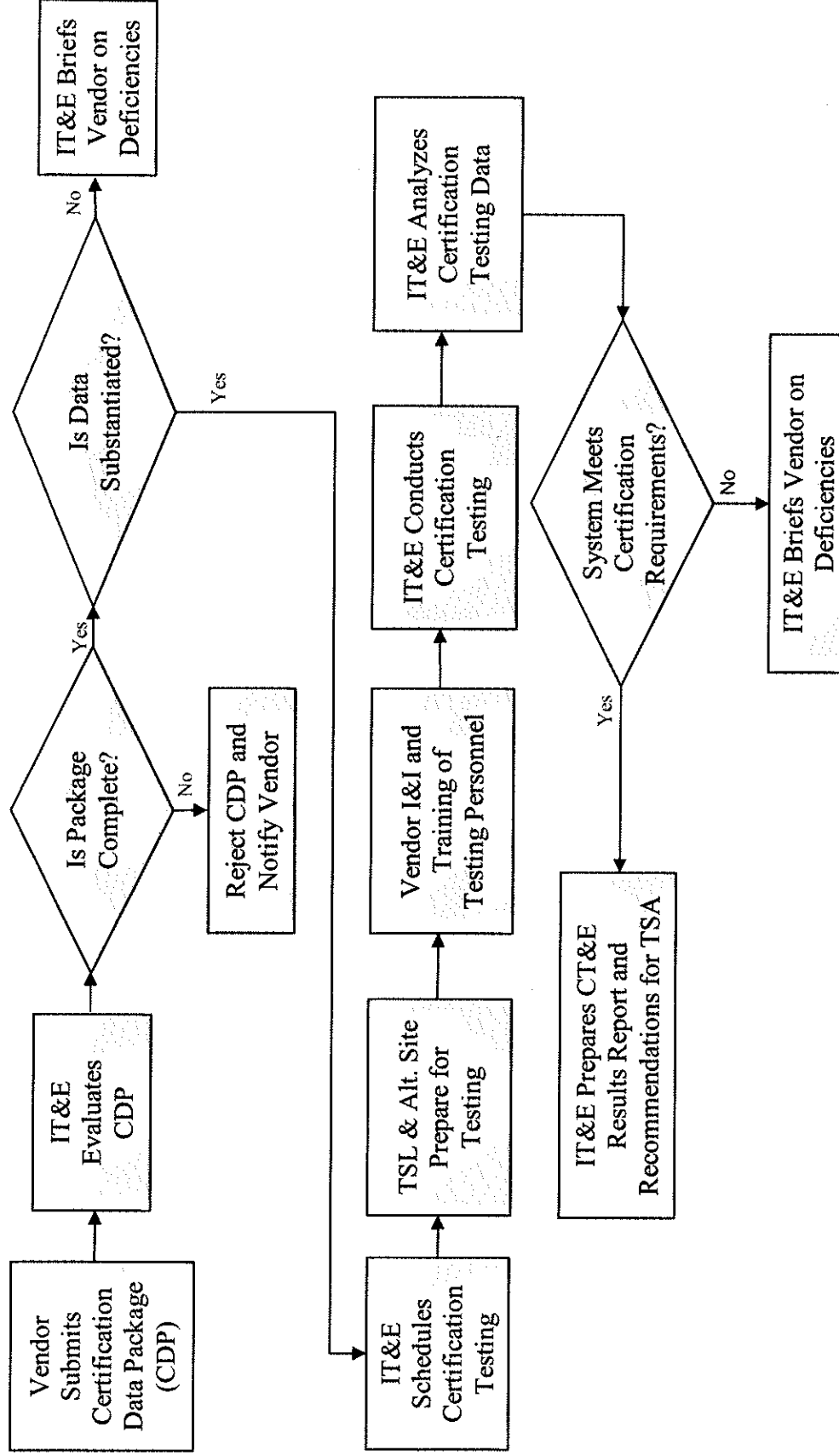


Figure 1: CPSS CT&E Overview

Management Plan for the CT&E of Checkpoint Property Screening Systems (CPSS)

1.2.1 Certification Readiness Testing

Certification Readiness Testing (CRT) is an optional process administered by the TSL's Developmental Test and Evaluation (DT&E) division that may indicate that a candidate CPSS may be accepted for CT&E. A candidate CPSS may also be accepted for CT&E based on alternative data provided in a CDP.

CRT is a combination of live scans and image replays that evaluate the system's ability to detect required objects and materials under a variety of conditions. During CRT, the DT&E team will evaluate the system's strengths and weaknesses for the detection of conventional explosives and homemade explosives (HME) configured in a variety of concealments. The team will also perform a Critical Excursion Test to probe for weak points in the system's detection capabilities. The candidate system must meet a predetermined level of detection and false alarm (FA) performance to move on to certification. These predetermined performance levels will be applied equally to all candidate systems. In addition, the system must show no detection gaps in its CRT Critical Excursion Test results, as determined by the IT&E Test Director.

1.2.2 Vendor Request for Certification Testing

Vendors may submit a request for CPSS Certification Testing to the Director of the T&E Division, TSA office of APM and/or to the IT&E Test Director. The vendor shall also submit a CDP to the IT&E Test Director, prepared in accordance with the instructions stated in this Management Plan. The CDP shall meet all the requirements outlined in Section 2 of this document and shall be electronically delivered to:

William Petracci (Test Director) at William.Petracci@HQ.DHS.GOV and
Anthony Vendetti (IT&E CPSS Test Lead) at Anthony.Vendetti@HQ.DHS.GOV

Vendors must submit a complete CDP, as defined in Section 2 "Vendor Instructions and CDP Requirements," or the entire package will be returned.

1.2.3 Evaluation of Vendor Certification Data Package

CDPs will be reviewed and evaluation reports prepared in the order data packages are received. The IT&E team will review the CDP and decide whether the package is to be approved or returned to the vendor because of incomplete or unsubstantiated data. The candidate CPSS used as a basis for the CDP must be a production or production-representative system and not specifically developed, selected, or tuned for certification testing purposes.

Test data will be examined for sufficiency, accuracy, validity, and substantiated detail. Additionally, the vendor's measurement techniques, CM practices, and test methodologies will be evaluated. The primary objective of the evaluation is to determine if the candidate CPSS has the potential to meet the CT&E criteria.

The IT&E team will prepare a report documenting the evaluation results within 30 days of CDP receipt. CDPs will be evaluated sequentially and not in parallel. Certification testing will only begin after approval of a CDP.

All company proprietary data shall be marked accordingly by the vendor at the time of CDP delivery. The TSL has instituted procedures to safeguard all company proprietary data contained within CDP submissions.

1.2.4 CPSS Installation and Integration (I&I)

The vendor shall ship one candidate CPSS to the TSL and a second candidate CPSS to an alternative Government-approved facility. The systems shall have the same configurations with respect to components that could affect detection performance, including system hardware, software, and tuning parameters. No system modifications will be allowed after the certification testing has been initiated without the written approval of the IT&E Test Director.

The vendor shall install and integrate (I&I) the candidate CPSS at the test facilities, in coordination with facility personnel. I&I shall include verification that the candidate CPSS meets all safety standards specified in this Management Plan, is functioning properly, and is in the proper configuration. System integration with external devices, such as baggage handling equipment or storage media, will also be accomplished during I&I. IT&E will observe vendor activities during this phase at both test locations.

1.2.5 Emulator Installation and Acceptance

The vendor shall ship one stand-alone offline emulator of the candidate CPSS to the TSL. The emulator shall be capable of reinterpreting the image data from saved live scans using the same algorithm presented for certification.

To ensure CM, the vendor is responsible for confirming to IT&E that the detection algorithm used by the emulator is the same as the algorithm used on the candidate CPSS. It is recommended that the medium used to install the detection algorithm software on the candidate CPSS also be used to install the detection algorithm software on the emulator. The vendor shall provide technical training to IT&E on the operation of the candidate CPSS and its emulator, including how to purge test and image data recorded on them. To be accepted, an emulator shall provide the same results as its associated system for any set of system-recorded images. A repeat acceptance test may be required if the reconstruction and/or detection algorithms undergo approved changes. IT&E will complete acceptance testing prior to initiation of certification testing.

To be accepted for CT&E by IT&E, the emulator must comply with the following requirements:

- a. The CPSS emulator shall be able to display and manipulate images that have been collected, stored, and downloaded to an external data storage device by the candidate CPSS;
- b. The user interface shall have all the same image enhancements and manipulation capabilities as the candidate CPSS;
- c. Vendors shall provide instructions and technical support, as needed, to allow images to be collected and stored from the candidate CPSS onto an external data storage device, and then loaded onto the emulator for display;
- d. Vendors shall provide instructions and a means to back-up, restore, and purge image data from the candidate CPSS and the emulator; and
- e. Administrative rights on the candidate CPSS and emulator shall be made available to IT&E to allow the verification of the removal of images, log files, and any other data collected during Certification Testing.

Management Plan for the CT&E of Checkpoint Property Screening Systems (CPSS)

1.2.6 Emulator and System Training

Once a candidate CPSS has been accepted for certification testing, the IT&E Test Director will contact the vendor to establish a schedule for IT&E training and familiarization at the TSL and the alternative Government-approved facility. These training and familiarization activities will be scheduled in the order in which installations of the candidate CPSS and emulator are completed. Training must be to the level which is necessary and sufficient to enable IT&E to perform all required activities, including certification testing and the purging of data. Following the completion of training and familiarization, and prior to certification testing, IT&E will prepare specific standard operating procedures for each candidate CPSS and emulator.

1.2.7 Configuration Management (CM)

Candidate CPSS and emulator CM and problem tracking will be established and maintained throughout the CT&E process, beginning with the submission of the vendor CDP. Hardware, software, and tuning parameter settings of each subsystem, including make, model, and revision level, shall be controlled and maintained by the vendor and reported to IT&E. IT&E will closely monitor CM during all activities, including physical configuration audits (PCA). PCAs will be administered upon the successful completion of I&I of the systems. The vendor shall submit all candidate CPSS and emulator proposed configuration changes to the IT&E Configuration Manager via a Developmental Engineering Proposal (DEP). The Configuration Manager will then inform the IT&E Test Director of the proposed modifications. A DEP must be approved before the proposed system modifications are implemented on a system under configuration control. Approval of any changes will be at the discretion of the IT&E Test Director.

The system configuration must reflect what is expected to be used in an airport screening environment. Specific tuning of the system to pass certification testing is prohibited. Candidate CPSS will only be tested by running one detection algorithm version at a time. Multiple versions of the same detection algorithm with adjustments to variable parameters or adaptation data will not be authorized for a single test event.

1.2.8 Pre-Certification Test and Evaluation

Following the successful completion of the vendor I&I and equipment training, pre-certification testing may be conducted at the discretion of the IT&E Test Director. The decision to perform this testing shall be made based on vendor or DT&E provided data. Pre-certification testing is an exploratory evaluation of the detection capabilities of a candidate CPSS. This testing may be divided into two (2) parts, conventional explosives and HME, and is focused on known system weaknesses and common points of failure that may have been observed during earlier test events. For a candidate CPSS to enter certification testing it must successfully demonstrate the potential of meeting TSA criteria for both conventional explosives and HME.

1.2.9 Certification Testing

The certification test is the formal test is administered to all candidate systems under the strictest control possible. IT&E will conduct certification testing using the test procedures developed for CPSS certification. Testing will be conducted under realistic operating conditions in accordance with the *Test Plan for Certification Test and Evaluation of Checkpoint Property Screening Systems (CPSS)* [1]. The same test set will be utilized for the certification testing of all candidate CPSS.

Management Plan for the CT&E of Checkpoint Property Screening Systems (CPSS)

The vendor shall not be allowed to witness certification tests. Data recording (logging) of test events or test objects by the candidate CPSS or emulator for vendor use is prohibited. If recordings are made, they will become the property of the TSA and shall be purged upon completion of the testing.

The vendor may be called upon for technical and maintenance support during certification testing, as required. All CPSS malfunctions or anomalies encountered during the CT&E process, will be documented in a test observation or problem report, classified by type, and tracked by IT&E. Problems and anomalies will be reviewed with the vendor for resolution and any required corrective actions.

CT&E will be terminated if the candidate CPSS or emulator malfunctions and cannot be repaired or replaced within three working days, unless the IT&E Test Director approves additional time. IT&E may perform retest or regression testing of a candidate CPSS or emulator to verify the integrity of the system following a repair, replacement of parts, or any software modifications. Configuration changes may result in rescheduling of the test.

The vendor is responsible for the removal of the candidate systems and emulator following an unresolved malfunction, rescheduling of certification testing, or at the conclusion of a failed certification test. Removal shall be at the discretion of the Test Director and completed within one week from notification.

Disposition of candidate systems and emulators that passed certification testing shall be at the discretion of the TSA, in consultation with the vendor and the Test Director.

1.2.10 Reporting of Results and Certification Recommendation

Following conclusion of certification testing, IT&E will prepare a report of CT&E results. This classified as secret, will include a summary of test events and all test results. This report, will be provided to the Director of the T&E Division, TSA office of APM. Prior to completion of the final report, a quick look report (QLR) may be provided to the TSA office of APM at their request.

If a candidate system meets or exceeds certification requirements, a recommendation for certification will be provided by the IT&E Test Director to the Director of the T&E Division, TSA office of APM, and to the Assistant Administrator of the TSA office of RCA.

If a candidate system does not meet certification requirements, the Test Director will brief the vendor on performance deficiencies. This briefing will be limited in nature, consisting of a qualitative description (Strong, Acceptable, Weak) of each explosive category detection performance. For any explosive category that failed to meet the required detection performance, the detection rate (DR) results will be rounded up or down to the nearest 10 percent. Measured rates for overall detection and FA will also be provided. Test results and sensitive data from IT&E related to the deficiency briefing will only be provided to vendor personnel on a need-to-know basis.

To resubmit a candidate CPSS for CT&E all deficiencies must be corrected. The resubmission must follow the same process as the original submission. An amended CDP shall be submitted, evaluated, and approved by IT&E before an updated candidate CPSS is installed. The updated CDP shall provide evidence that the resubmitted CPSS meets all performance requirements, including those previously failed.

Management Plan for the CT&E of Checkpoint Property Screening Systems (CPSS)

All test documentation will be classified, as appropriate, in accordance with the *Department of Homeland Security S&T Explosives Research & Development Program Security Classification Guide (March 2018)* [2].

1.2.11 Certification Process Schedule

The CT&E process period is estimated to consist of the following:

- a. Evaluation of CDP (four weeks);
- b. Vendor system I&I and training of the CT&E team (two weeks);
- c. Pre-certification testing (two weeks);
- d. Certification testing (six weeks);
- e. Notification to vendor and TSA office of APM of data analysis results (within one week of test completion);
- f. Preparation of Quick Look Report (one week);
- g. Briefing on test results to vendor (within two weeks of test completion); and
- h. Issuance of Final Report on CPSS that pass certification testing to the Director of the Test and Evaluation Division, TSA office of APM (within four weeks of test completion).

1.3 Organizational Roles and Responsibilities

1.3.1 TSA office of APM

- a. Review and approve this *Management Plan for Certification Test and Evaluation of Checkpoint Property Screening Systems (CPSS)*;
- b. Review and approve the *Test Plan for Certification Test and Evaluation of Checkpoint Property Screening Systems (CPSS)*;
- c. Review and approve the *Emulator Validation Plan for Certification Test and Evaluation of Checkpoint Property Screening Systems (CPSS)*;
- d. Performs prohibited item (PI) CT&E; and
- e. Issuance of Certification letter.

1.3.2 IT&E Test Director (TSL)

- a. Develop and distribute this *Management Plan for Certification Test and Evaluation of Checkpoint Property Screening Systems (CPSS)*;
- b. Develop the test plan and procedures for CPSS CT&E;
- c. Develop, document, and maintain test sets;
- d. Ensure proper safeguarding of all documents containing classified and company propriety information;
- e. Perform baseline configuration audits;
- f. Evaluate vendor CDPs and prepare evaluation reports;
- g. Schedule, coordinate, and conduct CPSS CT&E;
- h. Perform data reduction and analysis of test results;
- i. Develop test reports and issue recommendations; and
- j. Brief CPSS vendors on the CDP evaluation and certification test results.

1.3.3 Alternative Government-Approved Test Facility Lead

- a. Control the HME test article set;
- b. Maintain configuration control of candidate systems; and
- c. Execute HME data collection activities.

2. Vendor Instructions and Certification Data Package (CDP) Requirements

2.1 Purpose

The purpose of this section is to specify the preparation instructions, contents, and format of the CDP, which shall be submitted to the IT&E Test Director. For systems previously submitted for certification, vendors shall submit in accordance with Section 2.5.6.

The CDP shall contain all required information and be prepared in a manner that is clear, concise, and unambiguous. All materials shall be submitted in English and shall include a copy of the request for CPSS Certification submitted to the TSA, along with the CPSS Level, as defined in reference 5, against which the system's detection capability is to be assessed (Level 0, 1, 2, or 3). If the government tests at a level that was not declared, the vendor will be given credit for passing results. For example, if a system is declared at Level 0 and the government proceeds to test at Level 1, the system will receive certification for its Level 1 capabilities. Likewise, if a system is declared at Level 1 and the government tests at Level 0, the system will receive certification for its Level 0 capabilities.

Vendors shall use Proprietary and Sensitive Security Information (SSI) markings according to standard marking procedures. SSI shall be handled according to 49 CFR 15 and 1520. The CDP shall not contain any classified data (submitted test data shall be coded and submitted separately). The TSL has instituted procedures to safeguard proprietary data used during the CDP evaluation and throughout the CT&E process. The CDP will become a part of the official records of compliance testing for each CPSS model submitted.

2.2 Identification of Systems and Emulator

The vendor shall provide unique and complete identification of all systems and emulators. This includes systems used to collect test data, the CPSS systems installed at the TSL and alternative Government-approved facility, and the CPSS emulator installed at the TSL. Locations of the systems shall be provided, and any differences between the CPSS to be provided for certification testing and the CPSS used to collect test data shall be noted. Details which must be provided include:

- a. Model number(s);
- b. Serial number(s);
- c. Software version(s), including version of software subcomponents, such as reconstruction and inspection;
- d. A detailed component listing of hardware, software, and firmware configurations; and
- e. Identification of all configurable and adjustable parameters and adaptation data used to tailor or tune the system, as well as their settings and values. Adaptation data refers to variables used to configure or adjust the system to specific environments or uses. Note: This is only for settings and values which are relevant to the system's image quality and

Management Plan for the CT&E of Checkpoint Property Screening Systems (CPSS)

detection performance and does not need to include those parameters under configuration control as part of system reconstruction and detection software.

2.3 Theory of Operation

The vendor shall describe the CPSS principles of operation, along with all functional and performance capabilities. The vendor shall also provide detailed answers to the following questions if machine learning has been implemented into the proposed system or algorithm.

- a. For what detection tasks or threats are machine learning algorithms used?
- b. Are different algorithms used for different detection tasks or threats, or do multiple algorithms ensemble together to make a single decision?
- c. Is classical machine learning or deep learning employed?
 - i. If classical, what type of architecture is used and what are the input features?
 - ii. If deep learning, what architecture does the neural network follow?
- d. What was the number of images used per detection class for training, validation, and testing?
- e. What are the sources of the training, validation, and testing data? Describe how test data are different than the training or validation data.
- f. Was any synthetic data used for training or testing?
 - i. How were these data validated?
 - ii. How were these data used (e.g., training, validation, or testing)?
- g. Has any sensitivity training or testing been performed with respect to system variants (e.g., lower voltage, old x-ray tube)?

2.4 Safety

Substantiation shall be provided to demonstrate that candidate CPSS submitted for testing meet the safety requirements contained in:

- UL 61010-1, *Electrical Equipment for Measurement, Control, and Laboratory Use; Part 1: General Requirements, 2nd edition, revised: May 2012* [3]. The vendor shall provide a third-party certification report from an approved nationally recognized test laboratory (NRTL). A UL Field Evaluation certificate performed on a single system is acceptable.
- FDA 21 CFR 1020.40, *Performance Standards for Ionizing Radiation Emitting products, Cabinet X-Ray Systems, revised April 1, 2015* [4]. The vendor may self-certify against this requirement.

2.5 Data Requirements

The CDP shall include all information specified in either Section 2.5.1 or Section 2.5.6 below, as appropriate. These data are necessary to demonstrate the CPSS has a reasonable likelihood of meeting the certification criteria specified in *TSA Accessible Property Screening System (APSS) Detection Requirements* [5].

2.5.1 Data Requirements for Candidate CPSS Not Previously Accepted for Certification Testing

2.5.1.1.1 System Level Documentation and Description

Management Plan for the CT&E of Checkpoint Property Screening Systems (CPSS)

It is understood that systems presented for certification testing may be in various stages of development and not all information described in this section may be available. It is strongly recommended that if the information described in this section is available, it be provided to allow for a thorough evaluation of the CDP. It will be at the discretion of the IT&E Test Director to determine whether sufficient system level documentation and description have been provided.

2.5.1.1.2 System Hardware Overview

The vendor shall list the major system hardware components, manufacturer, and model or part numbers.

The vendor shall provide a table detailing a product configuration baseline. Table 1 is a sample table and provided for illustrative purposes only. The table is to be based on the system's major components and critical items and may be altered to include each system's unique components.

Table 1. Product Configuration Baseline Matrix—Hardware

Item No.	Description	Location	Manufacturer Name	Model Number
	X-Ray Subsystem			
	X-ray Tank			
	High Voltage Power Supply			
	Data Acquisition System			
	Detector Array			
	ADC Converter			
	Collimator Assembly(s)			
	Data Link Receiver Assembly			
	Brush Assembly			
	Slip Ring			
	Air Conditioning Unit			
	Motion Control Subsystem			
	Conveyor Gear Assembly			
	Conveyor Motor Controller			
	Conveyor Belt Assembly			
	Gantry Motor Assembly			
	Data Processing Subsystem			
	Host Computer			
	Reconstruction Computer			
	Inspection/Algorithm Computer			
	Operator Workstation			
	Image Quality Test Kit			

2.5.1.1.3 System Software Overview

The vendor shall provide a comprehensive explanation of the system software and their functions within the system. The system software overview shall include items such as system diagrams and a table listing the system software components with their version number. The following items and information shall also be included:

Management Plan for the CT&E of Checkpoint Property Screening Systems (CPSS)

- a. A list of detection-critical files and corresponding location/path on the CPSS system/component;
- b. Detailed software verification procedures (can be provided as attachments or appendices); and
- c. Software installation procedures (can be provided as attachments or appendices).

The vendor shall provide a table detailing the configuration baseline of the candidate CPSS. Table 2 is provided for illustrative purposes only and may be altered to describe each system's unique components.

Table 2. Product Configuration Baseline—Software

Item No.	Description	Version
	Release/Application/Host Software	
	Detection Computer System	
	Operating System	
	Detection Software	
	Firmware Versions	
	Reconstruction Computer System	
	Operating System	
	Reconstruction Software	
	Firmware Versions	
	Workstation/Primary Viewing System	
	Operating System	
	System Software	
	Firmware Versions	
	Network Components	
	Firmware/Revision Versions	
	Image Quality Kit Software	

2.5.1.2 System CM Plan and Practice

The vendor shall provide documentation describing the system CM and QA plans and practices applied during system development, production, and T&E. This shall include the methods used for Configuration Identification, Configuration Control, Configuration Status Accounting and Configuration Audits of hardware, software, firmware, and tuning parameter settings. Vendors may submit evidence of ISO 9001:2008 quality standard certification or the Carnegie Mellon University Capability Maturity Model (CMM) Level 3 certification in lieu of CM and QA documents. Inclusion of recent independent and qualified third-party quality system audits must substantiate these quality certifications. IT&E reserves the right to contact the third-party auditors to request vendor quality and CM documents at any time.

2.5.2 Data Management Procedures

The vendor shall provide detailed information on, and procedures for, data collection, data location and storage, data retrieval, data deletion, and image playback. Detailed descriptions of the data collection and where the data are stored shall be provided. The following information shall be supplied:

- a. Detailed procedures to enable or disable data collection;
- b. Locations and paths for all data files, including reconstructed images, raw data, algorithm log files, error log files;
- c. Detailed procedures to retrieve data for each system component;
- d. Detailed procedures to delete all collected data from the system; and
- e. Detailed procedures for image playback, including a list any hardware or software required for the process.

2.5.3 Test and Evaluation Data

2.5.3.1 Minimum T&E Data Requirement

The vendor shall submit all T&E data. At a minimum, T&E data shall include all data the vendor used to demonstrate the CPSS has the potential of meeting the certification criteria. All data relative to DR and false alarm rate (FAR) must be collected using the same system configuration as it applies to detection performance.

2.5.3.2 Airport Data

The TSA office of APM will assist vendors, to the extent possible, in coordinating the selective placement of CPSS in airports for data collection prior to certification testing. For initial certification, the test data submitted to IT&E shall include FA data from a minimum of 5,000 stream-of-commerce accessible personal items at passenger checkpoints. Items shall include both bins and bags and other items placed directly on a conveyor belt. Each bin shall be considered a single item. The FA data shall establish an overall FAR, a FAR for items placed directly on a conveyor belt, and a FAR for bins. The lane concepts of operations (CONOPs) and bin type(s) shall be specified. Any CDP that does not contain this information will be rejected.

2.5.3.3 Laboratory T&E

The vendor shall submit a test plan that defines the vendor's approach, strategy, and T&E activities performed in the laboratory. The test plan shall include, but is not limited to, the following:

- a. Overall test approach;
- b. QA and CM practices and procedures;
- c. Test article descriptions, including:
 - i. total number of items and item characteristics; and
 - ii. total number of threats, including type, amount and shape of explosives and/or explosives simulants, location of threats, the methodology used for placing threats in the concealed items, and any other data relevant to the specific test objects;

- d. Rationale for test article selection and preparation methods;
- e. Simulant description, preparation and validation (if applicable); and
- f. Data analysis approach, including the analysis methods and calculations performed.

2.5.4 Simulants/Explosives Validation Data

The vendor shall provide validation data for all simulants used during testing, if other than TSL-issued simulants. Simulant validation data shall include measured characteristics of both the explosive and its replicated simulant. Sufficient data shall be provided to enable IT&E to verify the simulants used accurately represent the explosive characteristics being measured by the CPSS. Each specific simulant that was validated for use during the vendor testing shall be identified via some unique numbering or coding method for individual tracking purposes.

2.5.5 T&E Report

The vendor shall provide a T&E report that contains, at a minimum, the following information:

- a. Description of the test procedures;
- b. Summary of results and conclusion;
- c. Description of items screened;
- d. Description of threats used;
- e. System configuration;
- f. Operational belt speed;
- g. FAR observed for a minimum of 5,000 unique passenger bags/items;
- h. Any deviations from plans or procedures, anomalies observed during testing, or other problems encountered, as well as potential effect; and
- i. Specific data reduction and analysis performed, including specific statistical calculations and results for DR, and FAR, along with related data as defined in 2.5.3.

Test reports containing data on DR, FAR, and countermeasures linked to specific explosives are classified and shall be identified and handled accordingly. The use of the Explosives Code designated in TSA's Detection Standard should be used when an explosive code is required.

2.5.6 Data Requirements for Candidate CPSS Previously Accepted for Certification Testing

A CDP addendum is required before initiation of CT&E of any system previously accepted for certification testing. Reasons for filing a CDP addendum include failure of a previous certification test or configuration changes to a previously certified system. The addendum shall include the reason for filing the addendum, the changes made to the previously tested system, the expected results of the changes made, the reasoning justifying those expectations, and a Delta Detection Report, defined below.

The purpose of the Delta Detection Report is to identify trends in detection performance resulting from changes between a previously tested algorithm(s) and the one currently being submitted. The report must identify modified detection software and tuning parameters and describe changes to the detection logic. Expected and/or observed changes to detection and false alarm performance, based on these changes, must be discussed.

Management Plan for the CT&E of Checkpoint Property Screening Systems (CPSS)

Table 3 identifies specific test results that may be reported.

Table 3. Delta Detection Test Results

Explosive Category	Database Name	Number of Bags	DR and FAR for Previously Submitted CPSS	DR and FAR for CPSS to be Certified
Overall				

3. Reference Documents

- [1] – *Test Plan for Certification Test and Evaluation of Checkpoint Property Screening Systems (CPSS). TBD.*
- [2] – *Department of Homeland Security S&T Explosives Research & Development Program Security Classification Guide (March 2018).*
- [3] – UL 61010-1, *Electrical Equipment for Measurement, Control, and Laboratory Use; Part 1: General Requirements, 2nd edition, revised: May 2012.*
- [4] – FDA 21 CFR 1020.40, *Performance Standards for Ionizing Radiation Emitting Products, cabinet X-Ray Systems, revised April 1, 2015.*
- [5] – *TSA Accessible Property Screening System (APSS) Detection Requirements, Version 6.2, October 3, 2018.*