

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

TRANSPORTATION SECURITY ADMINISTRATION

OFFICE OF SECURITY TECHNOLOGY

PROCUREMENT SPECIFICATION FOR ADVANCED IMAGING TECHNOLOGY (AIT) FOR CHECKPOINT OPERATIONS

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 22202-4220

10 September 2009
FINAL, Version 2.1



U.S. Department of Homeland Security
Transportation Security Administration

Prepared By:
TSA Office of Security Technology

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Technical Report Documentation Page			
1. Report No. OST-ENG-AIT-PROCSPEC	2. Government Accession No. N/A	3. Recipient's Catalog No. N/A	
4. Title and Subtitle Procurement Specification for Advanced Imaging Technology (AIT) for Checkpoint Operations		5. Report Date 10 September 2009	
		6. Performing Organization Code TSA-16	
7. Author Office of Security Technology System Planning and Evaluation Group		8. Performing Organization Report No. OST-ENG-AIT-PROCSPEC	
9. Performing Organization Name and Address Transportation Security Administration Office of Security Technology System Planning and Evaluation 601 South 12 th Street Arlington, VA 22202		10. Work Unit No. (TRAIS) N/A	
		11. Contract or Grant No. N/A	
12. Sponsoring Agency Name and Address N/A		13. Type of Report and Period Covered FINAL	
		14. Sponsoring Agency Code DHS/TSA/OST/ENG/	
15. Supplementary Notes N/A			
16. Abstract This Procurement Specification establishes the technical requirements for the passenger Advanced Imaging Technology (AIT) system. AIT systems are passenger screening technologies which use imaging technology such as backscatter X-ray (BS) or millimeter-wave (MMW) to detect potential threats that may be hidden on a passenger or within their clothing			
17. Key Words		18. Distribution Statement This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520	
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 69	22. Price
Reproduction of completed page authorized			

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

DOCUMENT CHANGE HISTORY

b6

Version	Description – Author	Date
0.01	Initial Draft/ [REDACTED]	2/26/07
0.02	Revision [REDACTED]	3/7/08
0.03	Revision [REDACTED]	3/10/08
0.04	Template update and revision [REDACTED]	3/12/08
0.05	IPT Review Draft / [REDACTED]	3/14/08
0.06	IPT Comments Update [REDACTED]	3/28/08
0.07	Modified Detection Requirements, Tier format [REDACTED]	4/14/08
0.08	Modified Detection Requirements [REDACTED]	4/21/08
0.09	Modified layout / [REDACTED]	5/12/08
0.10	Comments Draft [REDACTED]	5/15/08
0.11	Incorporated Chief Engineer comments [REDACTED]	5/22/08
0.12	Updated detection requirements / [REDACTED]	6/10/08
0.13	Industry Comment Update [REDACTED]	7/2/08
0.14	OSO comments updated/ DSCI	8/14/08
0.15	Engineer team review	8/29/08
0.16	Formatting updates and detection requirement update	9/4/08
1.00	Finalized release	9/5/08
1.01	Updated RMA Section	9/22/08
1.02	Multiplexing requirement update/updated release	9/23/08
2.00	Change to Imaging Technology and Detection standard	7/17/09
2.1	Changed title and incorporated updates from the Question Tracker/ [REDACTED]	9/10/09

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

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 manufacturer's names appear herein solely because they are considered essential to the objective of this report. This document does not constitute Transportation Security Administration certification policy.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

TABLE OF CONTENTS

1.0	INTRODUCTION.....	1
1.1	BACKGROUND	1
1.2	SCOPE.....	1
1.3	SYSTEM DESCRIPTION.....	1
1.3.1	Major Components.....	1
1.4	DEFINITIONS.....	1
2.0	APPLICABLE DOCUMENTS.....	2
2.1	GENERAL.....	2
2.2	GOVERNMENT DOCUMENTS.....	2
2.3	NON-GOVERNMENT DOCUMENTS.....	2
2.4	ORDER OF PRECEDENCE.....	3
3.0	REQUIREMENTS.....	4
3.1	TIER I REQUIREMENTS	4
3.1.1	System.....	4
3.1.2	Electrical	10
3.1.3	Physical.....	10
3.1.4	Identification Markings.....	11
3.1.5	Environmental.....	11
3.1.6	Electromagnetic Compatibility	11
3.1.7	Human Factors.....	13
3.1.8	Regulatory.....	14
3.1.9	Reliability, Maintainability, and Availability	14
3.1.10	Safety	15
3.1.11	Security	16
3.2	TIER II REQUIREMENTS	17
3.2.1	System.....	17
3.3	TIER III REQUIREMENTS.....	17
3.3.1	System.....	17
3.4	OPTIONAL CAPABILITIES.....	18
3.4.1	Automated Threat Detection Marking	18
4.0	VERIFICATION	19
4.1	TEST AND EVALUATION	19
4.1.1	Developmental Test and Evaluation (DT&E).....	19
4.1.2	Qualification Testing	19
4.1.3	Operational Test and Evaluation (OT&E).....	19
4.1.4	First Article Test and Evaluation (FAT&E).....	19
4.1.5	Factory Acceptance Test (FAT).....	19
4.1.6	Site Acceptance Test (SAT).....	19

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

4.1.7	Continuous Assessment	19
4.2	VERIFICATION METHODS	20
4.2.1	Analysis	20
4.2.2	Demonstration.....	20
4.2.3	Inspection.....	21
4.2.4	Test.....	21
4.3	VERIFICATION REQUIREMENTS TRACEABILITY MATRIX.....	21
5.0	ACRONYMS.....	33
Appendix A	Transportation Security Equipment Information Technology Security Requirements	A-1
Appendix B	Field Data Reporting System Requirements	B-1
Appendix C	User Access Levels and Capabilities	C-1
Appendix D	TSA Operational Power Requirements	D-1
Appendix E	AIT Reports.....	E-1

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

1.0 INTRODUCTION

1.1 Background

The Department of Homeland Security (DHS), Transportation Security Administration (TSA), presents Advanced Imaging Technology (AIT) as a new device that is intended to be used to screen passengers.

1.2 Scope

This specification establishes the performance, design, and verification requirements for AIT systems.

1.3 System Description

AIT systems are passenger screening technologies which use imaging technology to detect anomalies on a passenger's body or within their clothing. The mission of the AIT system is to effectively screen passengers at airport checkpoints, while preserving the privacy of passengers.

The requirements within this Procurement Specification have been broken into a tiered system. The vendor has the choice to meet the requirements of different tiers: Tier I encompasses the core requirements that must be met; Tiers II and III describe stepped requirements that may be met. A higher level system must meet all the requirements of the tier below it: for example, a Tier III system must meet all Tier I, Tier II, and Tier III requirements. Requirements are denoted by the use of a bold, italic, *shall*.

1.3.1 Major Components

AIT systems consist of the following major components:

- Scanner
- Image Operator Station
- Screening Operator Station

1.4 Definitions

Anomaly	Any undivested objects including explosives, weapons and liquids.
Downloading	Retrieving data or information from the AIT system either locally or remotely.
Image Operator (IO)	The TSO responsible for reviewing the images and communicating to the SO the alarm status for each passenger.
Screening Operator (SO)	The TSO responsible for scanning and managing each passenger during the AIT screening process.
<i>Shall</i>	Bolded, italicized "shalls" are requirements that the vendors' submitted AIT systems must meet, in accordance with the tier system.
Transportation Security Officer (TSO)	Formerly known as Screeners or Operators, TSOs are the TSA personnel who operate the airport security checkpoint and conduct security screening of all persons and objects entering the secure area.
Uploading	Loading data or information into the AIT system either locally or remotely.
AIT System	The combined performance of the AIT system including the operator in the loop.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

2.0 APPLICABLE DOCUMENTS

2.1 General

The documents listed in this section are referenced in this specification. While every effort has been made to ensure the completeness of this list, document users are cautioned that they must meet all requirements of this specification, whether or not the applicable references are listed. The following specifications, standards, handbooks, documents, and drawings of the exact revisions listed below form a part of this specification to the extent noted herein.

2.2 Government Documents

5 USC 552	Freedom of Information Act, 1996
29 CFR 1910.7	Occupational Health and Safety Administration (OSHA): Occupational Safety and Health Standards; Definition and Requirements for a Nationally Recognized Testing Laboratory, 1 January 2007
29 CFR 1910.1096	OSHA: Occupational Safety and Health Standards; Ionizing Radiation, 1 January 2007
29 CFR 1910.1200	OSHA: Occupational Safety and Health Standards; Toxic and Hazardous Substances: Hazard Communication, 1 January 2007
47 CFR 15	Federal Communications Commission (FCC); Radio Frequency Devices, 1 October 2007
49 CFR 15	Transportation: Protection of Sensitive Security Information, 1 October 2007
49 CFR 1520	Transportation Security Administration (TSA); Protection of Sensitive Security Information, 1 October 2006
49 CFR 1544.403	TSA; Airport Operator Security: Air Carriers and Commercial Operators: Current Screeners, 1 October 2006
49 CFR 1544.405	TSA; Airport Operator Security: Air Carriers and Commercial Operators: New Screeners: Qualifications of New Screening Personnel, 1 October 2006
DOT/FAA/CT-03/05	Human Factors Design Standard for Acquisition of Commercial Off-the-Shelf, Non-developmental, and Developmental Systems (2003).
FIPS 197	Federal Information Processing Standard (FIPS) 197 Advanced Encryption Standard (AES)
	TSA classified detection appendix <u>Advanced Imaging Technology for Checkpoint Screening Operations</u> , Version 3.0, July 10, 2009

2.3 Non-Government Documents

ANSI C63.16-1993	Discharge Test Methodologies and Criteria for Electronic Equipment (1993)
ANSI/HPS N43.17-2002	American National Standard – “Radiation Safety for Personnel Security Screening Systems Using X-ray.”
EN 55022	Limits and Methods of Measurement of Radio Disturbance Characteristics of Information Technology Equipment (Radiated Radio Frequency (RF) Emissions).
IEC 60068-2-64	Environmental Testing, Part 2: Test Methods – Test Fh: Vibration, Broad-band Random (Digital Control) and Guidance, 28 May 1993

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

IEC 61000-4-3	Testing and Measurement Techniques. Radiated, radio frequency, electromagnetic field immunity test.
IEC 61000-4-4	Testing and Measurement Techniques. Electrical fast transient/burst immunity test.
IEC 61000-4-5	Testing and Measurement Techniques. Surge immunity test.
IEC 61000-4-6	Testing and Measurement Techniques. Immunity to conducted disturbances, induced by radio-frequency fields.
IEC 61000-4-8	Testing and Measurement Techniques. Power frequency magnetic field immunity test.
IEC 61000-4-11	Testing and Measurement Techniques. Voltage dips and interruptions.
IEC 61000-6-3	Electromagnetic Compatibility (EMC). Generic Standards. Emission Standard for Residential, Commercial, and Light-industrial Environments, 17 July 2006
IEEE C95.1-2005	Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz
UL 310	Standard for Electrical Quick Connect Terminals, 27 May 2003
UL 61010-1	Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use, Part 1: General Requirements, 12 July 2004
	International Commission on Non-Ionizing Radiation Protection (ICNIRP) Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields (up to 300 GHz). Health Physics 74 (4): 494-522; 1998

2.4 Order of Precedence

In the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes national and state laws and regulations unless a specific exemption has been obtained.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

3.0 REQUIREMENTS

3.1 Tier I Requirements

3.1.1 System

3.1.1.1 Detection/Imaging

3.1.1.1.1 System Detection

The Concept of Operations for the AIT system encompasses a scenario in which an Image Operator (IO) reviews the AIT scanned image and determines if an anomaly is present. For this reason, detection performance for the "AIT system" refers to performance corresponding to the overall performance of AIT imaging and the operator in the loop. The AIT *shall* (1) image passengers without requiring the removal of clothing beyond outerwear. Detection performance requirements are as follows:

3.1.1.1.1.1 Explosives

The AIT system *shall* (2) produce images to enable an operator to determine the presence and location of explosives.

3.1.1.1.1.2 Weapons

The AIT system *shall* (3) produce images to enable an operator to determine the presence and location of weapons,

3.1.1.1.1.3 Liquids

The AIT system *shall* (4) produce images to enable an operator to determine the presence and location of liquids

3.1.1.1.1.4 Other Anomalies

The AIT system *shall* (5) produce images to enable an operator to determine the presence and location of other anomalies

3.1.1.1.2 Privacy

TSA policy dictates that passenger privacy is maintained and protected during passenger screening. To ensure passenger privacy safeguards are in place, AIT systems will prohibit the storage and exporting of passenger images during normal screening operations. When not being used for normal screening operations, the capability to capture images of non-passengers for training and evaluation purposes is needed. To ensure that image capturing maintains passenger privacy, the AIT system will provide two distinct modes of operation: Screening Mode and Test Mode as defined in 3.1.1.3.1.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

During Screening Mode, the AIT system *shall* (6) be prohibited from exporting passenger image data, including via STIP. During Test Mode, the AIT system *shall* (7) not be capable of conducting passenger screening.

The AIT system *shall* (8) prohibit local storage of image data in all modes.

The AIT system *shall* (9) employ 256-bit encryption for image data in accordance with Federal Information Processing Standard (FIPS) 197 Advanced Encryption Standard (AES).

The AIT system *shall* (10) provide image filters to protect the identity, modesty, and privacy of the passenger.

Enabling and disabling of image filtering *shall* (11) be modifiable by users as defined in the User Access Levels and Capabilities appendix.

The AIT system *shall* (12) ensure that images viewed by the IO are not viewable by the SO.

The AIT system *shall* (13) provide a means for passengers to maintain a line of sight to their divested carry-on items during the screening process.

3.1.1.2 Throughput Rate / Capacity

The AIT system *shall* (14) have an imaging time of no greater than 10 seconds. Imaging time is defined from when the scan is initiated until the image is fully projected onto the Image Operator Control Panel (IOCP).

The AIT system *shall* (15) be able to scan passengers with a height of up to at least [REDACTED]. Passenger access to the AIT system imaging area *shall* (16) be no less than [REDACTED]. The AIT system *shall* (17) require passengers to be [REDACTED] from the system in order to complete a scan.

The imaging area of the AIT system *shall* (18) be dimensioned so that a person, as defined above, is able to attain the required poses that the vendor deems necessary for optimal performance without bumping against any part of the system.

3.1.1.3 General System

3.1.1.3.1 Modes of Operation

3.1.1.3.1.1 Screening Mode

The AIT system *shall* (19) provide a Screening Mode. The AIT system Screening Mode *shall* (20) be the normal mode of operation for screening passengers for anomalies.

3.1.1.3.1.2 Test Mode

For purposes of testing, evaluation, and training development, the AIT system *shall* (21) provide a Test Mode. The AIT system Test Mode *shall* (22) be the sole mode of operation permitting the exporting of image data. AIT system Test Mode *shall* (23) be accessible as provided in the User Access Levels and Capabilities appendix.

When in Test Mode, the AIT system:

- *shall* (24) allow exporting of image data in real-time;
- *shall* (25) prohibit projection of an image to the IO station;

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

- *shall* (26) provide a secure means for high-speed transfer of image data;
- *shall* (27) allow exporting of image data (raw and reconstructed).

3.1.1.3.2 Start-Up and Power-Down

The AIT SO station *shall* (28) have start-up and power-down procedures or functions at the Screening Operator Station (see Section 3.1.1.4.1 below) that *shall* (29), upon completion of start-up, display a login window.

The AIT IO station *shall* (30) display a login window upon completion of SO Station start-up.

The AIT system *shall* (31) provide messages to the SO and IO that inform them of the system status.

3.1.1.3.2.1 Cold Start-up

The AIT system *shall* (32) complete cold start-up procedures in five (5) minutes or less from a powered off/shutdown mode. Powered off/shutdown mode is defined as a state in which an AIT system has been turned off or shutdown, but is still connected to a power source.

3.1.1.3.2.2 Sleep/Standby

The AIT system *shall* (33) complete a Sleep/standby start-up procedure in three (3) minutes or less from sleep/standby mode. Sleep/standby mode is defined as a power conserving state in which an AIT system has been turned on but is not fully functional.

3.1.1.3.2.3 Login Process

The AIT IO station *shall* (34) require no more than thirty (30) seconds to complete the login process. The AIT SO station *shall* (35) require no more than thirty (30) seconds to complete the login process. The login process is defined as the time from when the TSO enters user information and password to the time the TSO is able to scan passengers.

3.1.1.3.2.4 Fault Reset

The AIT system *shall* (36) have a fault reset time, after the fault has been corrected, of no more than two (2) minutes from activation of the system fault reset to ready for operation.

3.1.1.3.2.5 Power-Down

The AIT system *shall* (37) complete a power-down procedure in five (5) minutes or less. Power-down is defined as the transition from operational mode to shut-down mode.

3.1.1.3.3 Calibration

If the AIT system employs a technology that requires recalibration over time, the system *shall* (38) employ a calibration process that culminates in a visible notification to clearly indicate to the SO whether the AIT system is correctly calibrated and ready/not ready to scan a passenger. The calibration process *shall* (39) take place as necessary in order to keep the system accurate to its qualified detection tier. The AIT system *shall* (40) provide a message indicating to the operator that re-calibration is necessary and *shall* (41) not allow passengers to be scanned by the system during the calibration process.

3.1.1.3.4 Emergency Stop

The AIT system *shall* (42) include a physical emergency stop (E-Stop) button with protective guards to prevent accidental initiation of an emergency stop. An E-Stop button *shall* (43) be located at the SOCP. When an E-Stop button is enabled anywhere on the system, the E-Stop location *shall* (44) be identified on

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

the SO and IO stations. Activation of the E-Stop button *shall* (45) render the AIT system incapable of scanning passengers.

3.1.1.3.5 Lock Down

The AIT system *shall* (46) have a lock-down mode so that when activated by the SO:

- (a) No portion of the system *shall* (47) move under power.
- (b) System *shall* (48) not allow any passengers to be screened.
- (c) System *shall* (49) not emit scanning source radiation
- (d) System *shall* (50) not disable the display monitor or any means of two-way communication.

3.1.1.3.6 Network Interface

The AIT system:

- (a) *shall* (51) possess an Ethernet network interface equipped with an RJ-45 connector.
- (b) *shall* (52) support full/half duplex data rates of 10/100 mega-bits per second to support future requirements.
- (c) *shall* (53) support Transmission Control Protocol / Internet Protocol (TCP/IP).

3.1.1.4 Operator Stations

3.1.1.4.1 Screening Operator Station (SO Station)

The SO station:

- (a) *shall* (54) not interfere with the TSO's visual contact with passengers and their belongings, nor should it impact a TSO's ability to view the front and back end of the unit.
- (b) *shall* (55) have an activation button to initiate a scan. The activation button, if tethered to the device, *shall* (56) provide a minimum of 3 meters of cable length so that the cord does not interfere with the operator's activities.
- (c) *shall* (57) provide a hard-wired, secure means of communication between IO and SO. An audible means *shall* (58) be provided to communicate anomaly presence and location. A visual indicator *shall* (59) provide the SO with notification regarding passenger status. A green status indicator *shall* (60) be used to denote when passenger is cleared. A red status indicator *shall* (61) be used to denote when passenger requires secondary screening. The IO *shall* (62) be provided a means to reset the status indicator. This IO/SO communication *shall* (63) not be discernible by others.

3.1.1.4.2 Image Operator Station (IO Station)

The AIT IO station *shall* (64) include an Image Operator Control Panel (IOCP), which consists of the IO console and any other necessary input devices.

The IO station *shall* (65) be operable at a distance up to 100m from the AIT system.

3.1.1.4.2.1 IOCP

The IOCP:

- (a) *shall* (66) permit only authorized users to log on to the system.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

- (b) *shall* (67) provide a means to indicate clear or suspect status of a passenger.
- (c) *shall* (68) provide all controls required for the IO to view images.
- (d) *shall* (69) provide image enhancement tools to have, at a minimum, the following image processing capabilities, each selectable by a single keystroke to support image review:
 - (i) Reverse image contrast from full negative to full positive
 - (ii) Zoom [REDACTED]

b2

3.1.1.4.2.2 IOCP Display Monitor

The IOCP *shall* (70) include one or more flat panel color displays each measuring a minimum of 17 inches diagonally.

Mounting for the flat panel displays *shall* (71) allow the display(s) to be placed directly in front of the user when the user is in his or her normal working position. The monitors *shall* (72) be adjustable so that the centers of the monitors range from 110 cm to 145 cm from the surface on which the operator is standing.

These values are based on a seat height of 60 cm and a viewing distance of 65 cm. Note that the required monitor heights can vary as a function of seat height and viewing distance. A summary of the eye height, viewing distance, and viewing angle variables used in determining monitor height are provided in the figure below.

3.1.1.4.2.3 Display Monitor Mounting

The height and location of the IOCP, monitors, seat, and other controls with which IOs will interface must be considered together, as they will comprise a single workstation from which the TSOs will perform their screening tasks.

The monitors and IOCP *shall* (73) be easily accessible (visually or physically, as appropriate) from seated position at a standard desk height 28in (71.12 cm) – 30 in (76.2 cm) workstation.

The display monitor mounting method:

- (a) *shall* (74) allow operators to adjust height, tilt, and viewing angle without requiring the use of tools.
- (b) *shall* (75) allow for continuous adjustment or in increments of no more than 25 mm
- (c) *shall* (76) enable adjustments to be accomplished by a single individual
- (d) *shall* (77) be adjustable to allow a viewing distance from the eye to the display that is not less than 330 mm
- (e) *shall* (78) be adjustable so that the line of sight from viewer eye level to the center of the screen is between 10° and 20° below horizontal.
- (f) *shall* (79) have the capability to tilt displays up or down between -5° and +20°, in 5° increments or continuously.
- (g) *shall* (80) be possible to swivel the display by a minimum of 20° to the left or right, in 5° increments or continuously, to accommodate for varying ambient lighting conditions

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

- (h) *shall* (81) allow the monitor(s) to be placed directly in front of the user when the user is in his or her normal working position.
- (i) *shall* (82) ensure that monitor positions are stable over time once a position has been set. There should be no sagging, drooping, tilting, etc.

3.1.1.4.2.4 Operator Display

The monitor *shall* (83) display or indicate, at a minimum, the following:

- (a) Current operational state of the AIT system.
- (b) Present operational state of the scanner
- (c) Critical system parameters which state the operation of the scanner and the complete AIT system.
- (d) Identification of the IO.
- (e) System error messages and diagnostic results.
- (f) AIT system's images.

3.1.1.4.2.4.1 Image Quality

The images *shall* (84) have the resolution necessary for the TSO at the IO station to visually identify any anomalies.

The flat panel display *shall* (85) have a manufacturer's luminance rating ≥ 150 cd/m².

3.1.1.4.2.4.2 Jitter and Motion Artifacts

The display monitor *shall* (86) exhibit no perceptible jitter or motion artifacts.

3.1.1.5 Field Data Reporting System

The AIT system:

- (a) *shall* (87) ensure that all data recorded in the Field Data Reporting System (FDRS) is an accurate record of the events required to be recorded, as specified in Appendix B, and that all data in each of the tables are captured and correlated throughout.
- (b) *shall* (88) collect FDRS data as identified in Appendix B.
- (c) *shall* (89) display FDRS reports identified in Appendix E on the IO monitor.
- (d) *shall* (90) provide User Access data according to the access levels defined in the User Access Levels and Capabilities appendix.
- (e) *shall* (91) make FDRS raw data available for downloading.
- (f) *shall* (92) make FDRS data reports available for downloading.
- (g) *shall* (93) provide internal storage so that data elements (as defined in Appendix B) are stored for a minimum of one (1) year without being overwritten.

3.1.1.5.1 Data Storage/Transfer

The AIT system *shall* (94) provide capabilities for data transfers via USB devices. These devices *shall* (95) provide connectivity to download FDRS data as described in 3.1.1.5 and to upload/download a user database as defined in 3.1.11.2. A high capacity read/write drive *shall* (96) be installed to permit data

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

uploads and downloads. All necessary software drivers and operating system services to support the data collection devices *shall* (97) be preinstalled and preconfigured.

3.1.1.6 Access Control

The AIT system *shall* (98) comply with the levels of access control as defined in the User Access Levels and Capabilities appendix.

3.1.1.7 Operational Test Kit (OTK)

The vendor *shall* (99) provide an OTK that will validate the AIT system is operating as required.

3.1.2 Electrical

The AIT system:

- (a) *shall* (100) be capable of operating on commercially available 120 VAC or 240 VAC power at 60 Hz with a +/- 10% voltage tolerance and up to a +/- 3% variance in frequency, at no more than 20 amp service for 120 VAC or 50 amp for 220 VAC.
- (b) *shall* (101) route the power and data cables (if applicable) to floor level.
- (c) *shall* (102) meet the input power requirements defined in Appendix D, TSA Operational Power Requirements.

3.1.2.1 Uninterruptible Power Supply

The AIT system *shall* (103) include an Uninterruptible Power Supply (UPS) to ensure automatic, orderly, and safe shut-down of AIT system equipment and to preserve data in the event of loss of electrical power. The UPS *shall* (104) provide an indicator to the operator when running on UPS power and *shall* (105) provide an indicator to the operator when the UPS battery requires replacement.

3.1.3 Physical

3.1.3.1 Floor Loading

The total floor loading of the AIT system *shall* (106) not exceed 416.04 kg/m² (85 lbs/ft²) based on the actual foot print dimensions. The point load (concentrated load) *shall* (107) not exceed 453.59 kg over a 193.55 cm square (1,000 lbs over a 30 in square) floor area. The vendor *shall* (108) indicate the number of support legs and pad size including the maximum actual load in pounds-per-square-in (psi) per leg.

3.1.3.2 Scanner

3.1.3.2.1 Footprint

The AIT system footprint *shall* (109) be less than 4 square meters.

3.1.3.2.2 Orientation

The AIT system *shall* (110) be configurable so that passengers may face left or right in relation to the entrance during scanning.

3.1.3.2.3 Height

The AIT system height *shall* (111) be less than 3 m.

3.1.3.2.4 Width

The AIT system width *shall* (112) be no greater than 2.25 m.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

3.1.4 Identification Markings

3.1.4.1 Identification Information

The AIT system *shall* (113) identify the following information (which *shall* (114) is located to be readable without disassembly of any hardware):

- (a) Manufacturer name.
- (b) Model.
- (c) Unique serial number.

3.1.4.2 Permanency and Legibility

Direct identification marking and identification plates, tags, or labels used *shall* (115) be as permanent as the life expectancy of the item and *shall* (116) be capable of withstanding the environmental tests and cleaning procedures specified for the item to which it is affixed. Legibility *shall* (117) be understood to mean that which allows ready human or machine readability, as applicable. Information contained on identification plates *shall* (118) be displayed in a color that contrasts to the color of the surface of the plate. Identification tag marking, when used, *shall* (119) be permanent to the extent required for use of the item. The minimum text character height *shall* (120) be 2.54 mm (0.1 inch).

3.1.5 Environmental

3.1.5.1 Operational Environment

The AIT system *shall* (121) be capable of operating between 0° and 32° Celsius (32° and 89.6° Fahrenheit) and 10% to 80% relative non-condensing humidity, without affecting performance.

3.1.5.2 Storage Environment

The AIT system *shall* (122) be capable of storage between -7 °C and 49 °C (19.4 °F and 120.2 °F) and 10% to 98% relative, non-condensing humidity. The AIT system *shall* (123) be capable of storage under these conditions for not less than 12 months, without resulting in any temporary or permanent degradation of AIT system's performance or appearance.

3.1.5.3 Vibration Immunity

System function degradation resulting from low-frequency (low frequency vibration will be defined from 0.1 to 30 hertz) vibration typically stemming from airport terminal sources (e.g., aircraft departures/landings, heavy foot traffic, electric carts, large heating, ventilation and air conditioning (HVAC) systems, subfloor bag conveyors, and outdoor truck traffic) *shall* (124) be prevented by compliance with IEC 60068-2-64, *Environmental Testing. Part 2: Tests – Test Fh: Vibration, Broadband Random and Guidance*, or equivalent test type.

3.1.6 Electromagnetic Compatibility

The AIT system:

- (a) *shall* (125) comply with ANSI C63.16-1993, *Discharge Test Methodologies and Criteria for Electronic Equipment* in the following aspects:
 - (i) Section 9.4 Contact Discharge at 2 kV and 4 kV.
 - (ii) Section 9.3 Air Discharge at 2 kV, 4 kV and 8 kV.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

- (iii) Assuming 8 to 10 equipment discharge test points plus coupling planes, positive and negative discharge waveform polarities.
- (b) **shall** (126) comply with IEC 61000-4-3, *Testing and Measurement Techniques. Radiated, radio-frequency, electromagnetic field immunity test* in the following aspects:
 - (i) 10 V/meter, 80 MHz to 1 GHz.
 - (ii) Four sides of Equipment Under Test (EUT), 1% steps, 2.8 sec. dwell. AM Mod., 80%, 1 kHz.
 - (iii) Performance Criteria A.
- (c) **shall** (127) comply with IEC 61000-4-4, *Testing and Measurement Techniques. Electrical fast transient/burst immunity test* in the following aspects:
 - (i) Alternating Current (AC) and Direct Current (DC) power ports at 0.5kV, 1kV, and 2kV.
 - (ii) Signal lines over 3 m at 0.25 kV, 0.5kV and 1kV.
 - (iii) Performance Criteria B.
- (d) **shall** (128) comply with IEC 61000-4-5 *Testing and Measurement Techniques. Surge immunity test* in the following aspects:
 - (i) AC power port at 2kV line to earth, 1kV line to line at 0, 90 and 270 deg.
 - (ii) DC power ports at 0.5 kV line to earth, 0.5 kV line to line.
 - (iii) Signal lines over 30 m at 1 kV line to earth.
 - (iv) Positive and negative polarity, 5 surges per mode of appearance.
 - (v) Performance Criteria A.
- (e) **shall** (129) comply with IEC 61000-4-6, *Testing and Measurement Techniques. Immunity to conducted disturbances, induced by radio-frequency fields* in the following aspects:
 - (i) 10 Vrms, 150 kHz to 80 MHz.
 - (ii) Power ports and signal lines over 3 m, 1% steps, 2.8 sec. dwell.
 - (iii) Performance Criteria A.
- (f) **shall** (130) comply with IEC 61000-4-8, *Testing and Measurement Techniques. Power frequency magnetic field immunity test* in the following aspects:
 - (i) 30 A/m, 50 or 60Hz.
 - (ii) Performance Criteria A.
- (g) **shall** (131) comply with IEC 61000-4-11 *Testing and Measurement Techniques. Voltage dips and interruptions* in the following aspects:
 - (i) 30% reduction for 0.5 periods (10 ms), Performance Criteria B.
 - (ii) 60% for 5 periods (100 ms), Performance Criteria C.
 - (iii) 60% for 50 periods (1 sec), Performance Criteria C.
 - (iv) 95% for 250 periods (5 sec), Performance Criteria C

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

3.1.6.1 Personal Electronic Devices

A Personal Electronic Device (PED) is defined to include any PED, which in the user non-operational mode utilizes electronic circuitry to maintain computer clock and data storage functions. An unpowered PED is defined to include any PED, including FLASH memory devices, which in the user nonoperational mode utilizes electronic circuitry to maintain computer clock and data storage functions. The AIT system vendor *shall* (132) provide a report indicating that the AIT system unit has, at a minimum, undergone testing in accordance with the European Committee for Electro-technical Standardization (CENELEC) Standard EN 55022, Limits and Methods of Measurement of Radio Disturbance Characteristics of Information Technology Equipment (Radiated RF Emissions), or equivalent test type.

3.1.7 Human Factors

Note: Reference the human factors standards in DOT/FAA/CT-03/05 HF STD-001 - Human Factors Design Standard: Acquisition of Commercial Off-the-Shelf Subsystems, Non-Developmental Items, and Developmental Systems (2003) for the following requirements.

All AIT components with a user interface:

- (a) *shall* (133) be operable by TSOs meeting personnel requirements specified in 49 Code of Federal Regulations (CFR) Parts 1544.403 and 1544.405 in terms of auditory and visual acuity, dexterity, English proficiency, and educational level (high school diploma, General Educational Development (GED), or a combination of education and experience).
- (b) *shall* (134) use a graphical user interface (GUI) that is viewable on the AIT system's display monitor and controlled through the IOCP.
- (c) During utilization of the AIT system :
 - (i) The system *shall* (135) take no more than one (1) second from the time that a soft key or icon is selected to the time the action is complete, or the operator receives feedback that the soft key or icon was successfully selected.
 - (ii) Labels, icons, and colors *shall* (136) be used consistently across displays.
 - (iii) Key strokes *shall* (137) not be buffered.
 - (iv) The system *shall* (138) display a message or icon (such as an hourglass icon) to indicate when the system is busy processing an operator-initiated or machine-initiated command.
 - (v) If the same function keys or icons are available on more than one screen, then those functions *shall* (139) appear in the same location across screens.
 - (vi) The system *shall* (140) indicate when a function or mode has been activated or deactivated on any screen or console. Functions are activated by command from the control panel. Modes are changed via menu selection.
 - (vii) Function keys and icons *shall* (141) be assigned a single function to the maximum extent practicable.
 - (viii) If an action requires the use of an embedded menu system or a multistep process, then there *shall* (142) be available at all times a menu selection, key, or icon that allows the operator to cancel the last action or return to the starting position.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

3.1.7.1 Noise

Audible noise levels produced by the AIT system *shall* (143) not exceed a time-weighted average of 70 dBA within 1 m from the AIT system over a 5 minute period.

3.1.8 Regulatory

3.1.8.1 Electromagnetic Emission Safety

The AIT system *shall* (144) comply with IEC 61000-6-3, Electromagnetic Compatibility (EMC). Generic Standards: Emission Standard for Residential, Commercial, and Light-industrial Environments, 17 July 2006.

3.1.8.2 Emission Control

All AIT system radio frequency emissions *shall* (145) comply with 47 CFR 15, Radio Frequency Devices.

3.1.9 Reliability, Maintainability, and Availability

3.1.9.1 Reliability

The AIT system *shall* (146) be designed to meet a minimum of 1000 hours Mean Time Between Critical Failure (MTBCF) in an airport operational environment. This is calculated using a 16 hour duty day.

A critical failure means that the system cannot be used operationally. A failure that prevents the equipment from performing its intended function is considered as a critical failure.

A non-critical failure means that the system can still perform its intended function until the next scheduled maintenance interval.

3.1.9.2 Maintainability

The AIT system *shall* (147) be designed to have a Mean Time To Repair (MTTR) of not more than 4 hours. MTTR is defined as follows:

$$\text{MTTR} = \text{Total Active Corrective Maintenance Time} / \text{Number of Maintenance Actions}$$

3.1.9.2.1 Maintenance Access

The AIT system *shall* (148) have a maintenance access capability that requires no more than 60.96cm (24in) of external clearance distance for performing scheduled or unscheduled maintenance actions. The maintenance doors *shall* (149) be either removable or sliding with a key lock and handles.

3.1.9.2.2 Scheduled (Preventive) Maintenance

The AIT system *shall* (150) have a Mean Time Between Maintenance Action (MTBMA) for scheduled (preventive) maintenance of not less than seven (7) days. The maintenance manual *shall* (151) specify all scheduled maintenance activities and the intervals of performance.

The AIT system *shall* (152) not require any custom tools for the performance of scheduled maintenance.

3.1.9.2.3 Unscheduled (Corrective) Maintenance

The AIT system:

Shall (153) be modular in design to allow easy removal and replacement of failed Line Replaceable Units (LRUs).

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

- (a) Must provide Built In Testing (BIT) diagnostic capabilities that:
- (i) *shall* (154) initiate on power-up.
 - (ii) *shall* (155) monitor system health in a non-interference (background) mode during normal operations.
 - (iii) *shall* (156) capture and report error and failure codes to the FDRS.
- (b) Must provide Fault Isolation Test (FIT) diagnostic capabilities that:
- (i) *shall* (157) be manually initiated by the TSO as a result of BIT or other system-generated error.
 - (ii) *shall* (158) identify the failed LRU with at least 90% accuracy.
 - (iii) *shall* (159) be at least 98% accurate when isolating the failed component to one of three LRUs.
 - (iv) *shall* (160) report the resultant error or failure codes to the user display and store the resultant error or failure codes on the system for later retrieval as part of the FDRS.

3.1.9.3 Availability

The AIT system *shall* (161) demonstrate an inherent availability (A_i) threshold of at least 99%. Availability *shall* (162) be computed as:

$$A_i = [MTBF / (MTBF + MTTR)] * 100\%$$

Where MTBF is the Mean Time between Failures and MTTR is the Mean Time to Repair.

$$MTBF = 1 / \text{Failure rate}$$

$$\text{Failure Rate} = \text{Number of failures} / \text{Total Operating Hours}$$

3.1.10 Safety

3.1.10.1 General

The AIT system *shall* (163) not expose operators, passengers, or maintenance personnel to hot surfaces over 43.9 degrees Celsius (111 degrees Fahrenheit).

3.1.10.2 Radiation

The AIT system *shall* (164) comply with ANSI/HPS N43.17-2002 American National Standard – “Radiation Safety for Personnel Security Screening Systems Using X-ray.”

The AIT system *shall* (165) comply with OSHA Standard, 29 CFR 1910.1096, Ionizing Radiation, 1 January 2007.

The AIT system *shall* (166) comply with Institute of Electrical and Electronics Engineers (IEEE), C95.1 – 2005, Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz, revision of C95.1-1991 (Active).

The AIT system *shall* (167) comply with International Commission on Non-Ionizing Radiation Protection (ICNIRP), Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields (Up to 300 GHz). Health Physics 74 (4): 494-522, April 1998.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

3.1.10.3 Electrical Safety

The AIT system:

- (a) *shall* (168) comply with UL 61010-1, *Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use, Part 1: General Requirements*, 12 July 2004.
- (b) *shall* (169) comply with UL 310, Standard for Electrical Quick Connect Terminals, 27 May 2003.

These standards are applicable to electrical equipment used in the workplace and require approval or certification by a National Recognized Test Laboratory (NRTL) listed by OSHA in 29 CFR 1910.7.

3.1.10.4 Ergonomic Safety

The AIT system:

- (a) *shall* (170) possess no sharp corners or edges that can puncture, cut, or tear the skin or clothing, or otherwise cause bodily injury.
- (b) *shall* (171) mount external wires, connectors, or cables in a manner which will prevent trip hazard, disconnection or damage by operators and passengers through incidental contact.
- (c) *shall* (172) possess no loose covers and cowlings.

3.1.10.5 Hazardous Materials

If hazardous materials are used in the AIT system, they *shall* (173) be identified, including their location and amount by weight or volume. A complete Material Safety Data Sheet (MSDS) *shall* (174) be developed and provided to meet the requirements of 29 CFR 1910.1200, OSHA Hazard Communication. The hazardous materials *shall* (175) be packaged or configured to not require the use of personal protective equipment (e.g., respiratory protection, eye and face protection, hand protection, protective clothing).

3.1.11 Security

3.1.11.1 Physical Security

The units are to be used in areas accessible to the public. The AIT system:

- (a) *shall* (176) provide the means to physically protect its sensitive components and controls.
- (b) *shall* (177) possess highly visible tamper-evident seals or alarms on assemblies that contain sensitive components/data.

3.1.11.2 Software Access

The AIT system:

- (a) *shall* (178) allow user access, password protection, and capabilities per the User Access Levels and Capabilities appendix.
- (b) *shall* (179) have a user database with a minimum capacity of 10,000 users. A user database is defined as the user ID and password combinations to access the system.
- (c) *shall* (180) through the use of a graphical user interface (GUI) or menu, allow the user to encrypt and export a user database.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

(d) *shall* (181) through the use of a GUI or menu, allow the user to import and decrypt a user database.

3.1.11.3 Information Technology Security

The AIT system *shall* (182) address the technology security requirements set forth in Appendix A.

3.2 Tier II Requirements

3.2.1 System

3.2.1.1 Detection/Imaging

3.2.1.1.1 System Detection

Detection performance requirements are as follows:

3.2.1.1.1.1 Explosives

The AIT system *shall* (183) produce images to enable an operator to determine the presence and location of explosives

3.2.1.1.1.2 Weapons

The AIT system *shall* (184) produce images to enable an operator to determine the presence and location of weapons,

3.2.1.1.1.3 Liquids

The AIT system *shall* (185) produce images to enable an operator to determine the presence and location of liquids

3.3 TIER III Requirements

3.3.1 System

3.3.1.1 Detection/Imaging

3.3.1.1.1 System Detection

Detection performance requirements are as follows:

3.3.1.1.1.1 Explosives

The AIT system *shall* (186) produce images to enable an operator to determine the presence and location of explosives

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

3.3.1.1.1.2 Weapons

The AIT system *shall* (187) produce images to enable an operator to determine the presence and location of weapons.

3.3.1.1.1.3 Liquids

The AIT system *shall* (188) produce images to enable an operator to determine the presence and location of liquids.

3.4 Optional Capabilities

3.4.1 Automated Threat Detection Marking

The AIT system *shall* (189) provide an automated detection highlighting function in meeting the tiered detection requirements.

Automated detection highlighting of anomalies *shall* (190) be coded red.

Automated detection highlighting *shall* (191) be bounded by a box indicating the location of the anomaly.

The AIT system *shall* (192) provide a means for the IO to toggle automated detection highlighting on and off.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

4.0 VERIFICATION

Unless otherwise specified within this document, verification will be accomplished through inspection, test, demonstration, and analysis. To support compliance with the requirements in this specification, inspection, test, demonstration, and analysis will be performed on an AIT system that is representative of the approved production design that has been placed under configuration control.

4.1 Test and Evaluation

Use of the test and evaluation process will assure that an AIT system has met the requirements of the AIT specification, associated interface requirements and control documents, and algorithm description. Requirements verification will be performed in accordance with the Contract Statement of Work (SOW) and this Specification. All testing will be conducted according to Government-approved test plans, test cases, and test procedures and will be witnessed by an authorized Government representative.

4.1.1 Developmental Test and Evaluation (DT&E)

Contractor DT&E testing comprises test and evaluation of the engineering design and developmental process that is conducted by incrementally determining the degree to which functional engineering specifications are attained. Verification will proceed from the unit level, through integrated verification of functional areas and interfaces within the complete system, to the complete system, in as near an operational configuration and environment as practical.

4.1.2 Qualification Testing

The Government will conduct testing to verify compliance to the requirements set forth in this specification.

4.1.3 Operational Test and Evaluation (OT&E)

The Government will conduct OT&E on production-representative systems to assess operational effectiveness and suitability when used by representative field TSOs in the intended operational environment.

4.1.4 First Article Test and Evaluation (FAT&E)

An FAT&E will be performed, as directed by the Government, on the Contractor's first production model to verify compliance with all technical contract requirements.

4.1.5 Factory Acceptance Test (FAT)

The Contractor will conduct an FAT at the factory on each system prior to delivery. FAT will verify that each system is manufactured to the Government-approved product baseline, that each system complies with technical contract requirements, and that no defects from the manufacturing process exist.

4.1.6 Site Acceptance Test (SAT)

The Contractor will conduct an SAT at the site on each system prior to its placement into operation. SAT will verify that each system is properly installed and configured, and that no defects remain from the transportation and installation processes.

4.1.7 Continuous Assessment

The Government will perform continuous assessment of fielded AIT systems to verify operational effectiveness, suitability, reliability, and availability of the equipment. Continuous assessment will

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

include collection of data from fielded AIT systems for the purpose of assessing field performance over time.

4.2 Verification Methods

All AIT system development will undergo test and evaluation to verify that the AIT system meets system specification requirements. The verification methods (analysis, demonstration, inspection, and test) described below are mandatory for AIT requirements verification.

4.2.1 Analysis

4.2.1.1 Hardware

Hardware analysis will encompass any or all of the following:

- (a) Engineering analysis is an engineering design function comprising study, calculation, or modeling of the known or potential failure modes and the reactions or interactions of the specified parts, materials, and the design configuration with the known function, performance and/or probable effects of the operational environments. This analysis is customarily used to verify margin when it is not desirable to test to failure.
- (b) Similarity analysis is a method applied to end-items or components that are identical in design and manufacturing processes to end-items or components that have previously been qualified to equivalent or more stringent requirements. This method can be applied to commercial, off-the-shelf/non-developmental item (COTS/NDI) equipment for the same manufacturer's models, based on the manufacturer's engineering specifications. For COTS/NDI equipment, the use of manufacturer's published materials that contain test conformance information relating to materials construction, commercial reliability test data, internal performance capabilities, and environmental conditions (heat, power consumption, etc.) are acceptable.
- (c) Validation of records analysis is a method of verification wherein manufacturing records are used to verify the compliance of concealed construction features or processes of manufacturing (e.g., Contractor items). This method will be applied to COTS equipment for the same manufacturer's models based upon the manufacturer's engineering specifications.

4.2.1.2 Software

Software analysis will encompass the processing of accumulated results and conclusions to provide proof that the verification of requirements has been accomplished. The analytical results may be composed of interpretation of existing information or derived from lower level tests, demonstrations, analyses, or examinations.

4.2.2 Demonstration

The demonstration method of verification is used to indicate a general "pass/fail" condition.

4.2.2.1 Hardware

Hardware demonstration will determine, by observation, the qualitative characteristics of end-item or component properties. Demonstration will require no special test equipment or instruction to verify characteristics such as operational performance, human engineering features, service, access features, and transportability.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

4.2.2.2 Software

Software demonstration will determine compliance with requirements (e.g., the proper response at a site as a result of a specified interrogation or command to be processed by the program) through observation of functional operation. Demonstration will be used primarily for activities where data gathering is not appropriate, such as display image verification.

4.2.3 Inspection

4.2.3.1 Hardware

Inspection of hardware will comprise verifying physical characteristics to determine compliance with requirements without the use of special laboratory equipment, procedures, items, or services. Inspection will verify workmanship, physical condition, construction features, and document/drawing compliance. For COTS/NDI hardware, use of manufacturer's published materials that contain test conformance information such as commercial reliability test data, safety regulations, or other Government standards and licensing, as applicable, are acceptable.

4.2.3.2 Software

Inspection will consist of an examination that comprises review of software source and object listings to verify compliance with software documentation, technical requirements, coding standards, and verification of the implementation of required algorithms.

4.2.4 Test

4.2.4.1 Hardware

Hardware testing will verify hardware performance during or after the controlled application of functional and/or environmental stimuli. The test equipment required for verification will be calibrated and kept in proper working condition. Any test hardware or software used will be documented, validated, and kept under configuration control.

4.2.4.2 Software

Software testing will employ technical means, including evaluation of functional operation by use of special equipment or instrumentation, software and/or simulation techniques, to determine compliance of the system with requirements. Data derived from software testing will be reduced for analysis of software/system performance under the test specified. Test equipment required for verification will be calibrated and in proper working condition. Any test hardware or software will be documented, validated, and under configuration control.

4.3 Verification Requirements Traceability Matrix

The Verification Requirements Traceability Matrix (VRTM) shown in Table I defines the verification method to be used to validate each AIT specification requirement. Formal verification tests will encompass the following range of conditions, when applicable:

- Normal data flow or condition.
- Minimum and maximum conditions.
- Below minimum and above maximum conditions.
- System failures and recovery.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

TABLE I. Verification Requirements Traceability Matrix

Req. #	Paragraph Number	Paragraph Title	FAT&E	FAT	SAT	Remarks
1	3.1.1.1.1	System Detection	D	D	D	
2	3.1.1.1.1.1	Explosives	A	X	X	Q-T
3	3.1.1.1.1.2	Weapons	A	X	X	Q-T
4	3.1.1.1.1.3	Liquids	A	X	X	Q-T
5	3.1.1.1.1.4	Other Anomalies	A	X	X	Q-T
6	3.1.1.1.2	Privacy	D	X	X	
7	3.1.1.1.2	Privacy	D	X	X	
8	3.1.1.1.2	Privacy	D	X	X	
9	3.1.1.1.2	Privacy	I	X	X	
10	3.1.1.1.2	Privacy	D	X	X	
11	3.1.1.1.2	Privacy	D	D	D	
12	3.1.1.1.2	Privacy	D	D	D	
13	3.1.1.1.2	Privacy	I	I	I	
14	3.1.1.2	Throughput Rate / Capacity	T	X	X	
15	3.1.1.2	Throughput Rate / Capacity	I	X	X	
16	3.1.1.2	Throughput Rate / Capacity	I	X	X	
17	3.1.1.2	Throughput Rate / Capacity	D	X	X	
18	3.1.1.2	Throughput Rate / Capacity	I	X	X	
19	3.1.1.3.1.1	Screening Mode	D	X	X	
20	3.1.1.3.1.1	Screening Mode	D	D	X	
21	3.1.1.3.1.2	Test Mode	D	D	X	
22	3.1.1.3.1.2	Test Mode	D	D	X	
23	3.1.1.3.1.2	Test Mode	D	D	X	
24	3.1.1.3.1.2	Test Mode	D	D	X	
25	3.1.1.3.1.2	Test Mode	D	D	X	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

26	3.1.1.3.1.2	Test Mode	D	X	X	
27	3.1.1.3.1.2	Test Mode	D	D	X	
28	3.1.1.3.2	Start-up and Power-Down	D	D	X	
29	3.1.1.3.2	Start-up and Power-Down	D	D	X	
30	3.1.1.3.2	Start-up and Power-Down	D	D	X	
31	3.1.1.3.2	Start-up and Power-Down	D	D	X	
32	3.1.1.3.2.1	Cold Start-up	D	D	X	
33	3.1.1.3.2.2	Sleep / Standby	D	D	X	
34	3.1.1.3.2.3	Login Process	D	D	X	
35	3.1.1.3.2.3	Login Process	D	D	X	
36	3.1.1.3.2.4	Fault Reset	D	D	X	
37	3.1.1.3.2.5	Power-Down	D	D	X	
38	3.1.1.3.3	Calibration	D	D	D	
39	3.1.1.3.3	Calibration	D	D	D	
40	3.1.1.3.3	Calibration	D	D	D	
41	3.1.1.3.3	Calibration	D	D	D	
42	3.1.1.3.4	E-Stop	I	I	X	
43	3.1.1.3.4	E-Stop	I	I	X	
44	3.1.1.3.4	E-Stop	I	I	X	
45	3.1.1.3.4	E-Stop	D	D	D	
46	3.1.1.3.5	Lock Down	D	X	X	
47	3.1.1.3.5	Lock Down	T	T	X	
48	3.1.1.3.5	Lock Down	T	X	X	
49	3.1.1.3.5	Lock Down	T	X	X	
50	3.1.1.3.5	Lock Down	T	T	X	
51	3.1.1.3.6	Network Interface	I	I	X	
52	3.1.1.3.6	Network Interface	A	X	X	
53	3.1.1.3.6	Network Interface	A	X	X	
54	3.1.1.4.1	SO Station	I	I	I	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

55	3.1.1.4.1	SO Station	I	I	X	
56	3.1.1.4.1	SO Station	I	X	X	
57	3.1.1.4.1	SO Station	I	X	X	
58	3.1.1.4.1	SO Station	D	D	D	
59	3.1.1.4.1	SO Station	D	D	D	
60	3.1.1.4.1	SO Station	D	D	D	
61	3.1.1.4.1	SO Station	D	D	D	
62	3.1.1.4.1	SO Station	D	D	D	
63	3.1.1.4.1	SO Station	D	D	D	
64	3.1.1.4.2	IO Station	I	X	X	
65	3.1.1.4.2	IO Station	D	X	X	
66	3.1.1.4.2.1	IOCP	T	X	X	C-C
67	3.1.1.4.2.1	IOCP	D	X	X	
68	3.1.1.4.2.1	IOCP	D	X	X	
69	3.1.1.4.2.1	IOCP	D	X	X	
70	3.1.1.4.2.2	IOCP Display Monitor	I	X	X	
71	3.1.1.4.2.2	IOCP Display Monitor	I	I	I	
72	3.1.1.4.2.2	IOCP Display Monitor	I	I	I	
73	3.1.1.4.2.3	Display Monitor Mounting	D	D	D	
74	3.1.1.4.2.3	Display Monitor Mounting	D	D	D	
75	3.1.1.4.2.3	Display Monitor Mounting	T	X	X	
76	3.1.1.4.2.3	Display Monitor Mounting	D	X	X	
77	3.1.1.4.2.3	Display Monitor Mounting	T	X	X	
78	3.1.1.4.2.3	Display Monitor Mounting	T	X	X	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

79	3.1.1.4.2.3	Display Monitor Mounting	T	X	X	
80	3.1.1.4.2.3	Display Monitor Mounting	T	X	X	
81	3.1.1.4.2.3	Display Monitor Mounting	D	D	D	
82	3.1.1.4.2.3	Display Monitor Mounting	I	I	I	
83	3.1.1.4.2.4	Operator Display	I	I	I	
84	3.1.1.4.2.4.1	Image Quality	I	I	X	
85	3.1.1.4.2.4.1	Image Quality	I	X	X	
86	3.1.1.4.2.4.2	Jitter and Motion Artifacts	I	X	X	
87	3.1.1.5	Field Data Reporting System	D	X	X	
88	3.1.1.5	Field Data Reporting System	D	X	X	
89	3.1.1.5	Field Data Reporting System	D	X	X	
90	3.1.1.5	Field Data Reporting System	D	D	X	
91	3.1.1.5	Field Data Reporting System	D	X	X	
92	3.1.1.5	Field Data Reporting System	D	X	X	
93	3.1.1.5	Field Data Reporting System	A	X	X	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

94	3.1.1.5.1	Data Storage / Transfer	D	D	D	
95	3.1.1.5.1	Data Storage / Transfer	D	D	D	
96	3.1.1.5.1	Data Storage / Transfer	I	I	X	
97	3.1.1.5.1	Data Storage / Transfer	I	X	X	
98	3.1.1.6	Access Control	A	X	X	
99	3.1.1.7	OTK	D	X	X	
100	3.1.2	Electrical	T	X	X	
101	3.1.2	Electrical	D	D	D	
102	3.1.2	Electrical	T	X	X	
103	3.1.2.1	Uninterruptible Power Supply	D	I	I	
104	3.1.2.1	Uninterruptible Power Supply	D	D	X	
105	3.1.2.1	Uninterruptible Power Supply	D	X	X	
106	3.1.3.1	Floor Loading	A	X	X	
107	3.1.3.1	Floor Loading	A	X	X	
108	3.1.3.1	Floor Loading	A	X	X	
109	3.1.3.2.1	Footprint	I	X	X	
110	3.1.3.2.2	Orientation	D	X	X	
111	3.1.3.2.3	Height	I	X	X	
112	3.1.3.2.4	Width	I	X	X	
113	3.1.4.1	ID Info.	I	X	X	
114	3.1.4.1	ID Info.	I	X	X	
115	3.1.4.2	Permanency and Legibility	A	X	X	
116	3.1.4.2	Permanency and Legibility	T	X	X	
117	3.1.4.2	Permanency and Legibility	A	X	X	
118	3.1.4.2	Permanency and Legibility	I	X	X	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

119	3.1.4.2	Permanency and Legibility	A	X	X	
120	3.1.4.2	Permanency and Legibility	I	X	X	
121	3.1.5.1	Operational Environment	A	X	X	C-C
122	3.1.5.2	Storage Environment	A	X	X	C-C
123	3.1.5.2	Storage Environment	A	X	X	C-C
124	3.1.5.3	Vibration Immunity	A	X	X	C-I
125	3.1.6	Electromagnetic Compatibility	A	X	X	C-I
126	3.1.6	Electromagnetic Compatibility	A	X	X	C-I
127	3.1.6	Electromagnetic Compatibility	A	X	X	C-I
128	3.1.6	Electromagnetic Compatibility	A	X	X	C-I
129	3.1.6	Electromagnetic Compatibility	A	X	X	C-I
130	3.1.6	Electromagnetic Compatibility	A	X	X	C-I
131	3.1.6	Electromagnetic Compatibility	A	X	X	C-I
132	3.1.6.1	PED	A	X	X	C-I
133	3.1.7	Human Factors	A	X	X	
134	3.1.7	Human Factors	D	X	X	
135	3.1.7	Human Factors	T	X	X	
136	3.1.7	Human Factors	I	X	X	
137	3.1.7	Human Factors	D	X	X	
138	3.1.7	Human Factors	I	X	X	
139	3.1.7	Human Factors	I	X	X	
140	3.1.7	Human Factors	I	X	X	
141	3.1.7	Human Factors	I	X	X	
142	3.1.7	Human Factors	D	X	X	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

143	3.1.7.1	Noise	T	X	X	
144	3.1.8.1	Electromagnetic Emission Safety	A	X	X	C-I
145	3.1.8.2	Emission Control	A	X	X	C-I
146	3.1.9.1	Reliability	A	X	X	C-C
147	3.1.9.2	Maintainability	A	X	X	C-C
148	3.1.9.2.1	Maintenance Access	I	I	X	
149	3.1.9.2.1	Maintenance Access	I	X	X	
150	3.1.9.2.2	Scheduled Maintenance	A	X	X	
151	3.1.9.2.2	Scheduled Maintenance	A	X	X	
152	3.1.9.2.3	Scheduled Maintenance	A	X	X	
153	3.1.9.2.3	Unscheduled Maintenance	I	X	X	
154	3.1.9.2.3	Unscheduled Maintenance	D	X	X	
155	3.1.9.2.3	Unscheduled Maintenance	D	X	X	
156	3.1.9.2.3	Unscheduled Maintenance	D	X	X	
157	3.1.9.2.3	Unscheduled Maintenance	D	X	X	
158	3.1.9.2.3	Unscheduled Maintenance	T	X	X	
159	3.1.9.2.3	Unscheduled Maintenance	T	X	X	
160	3.1.9.2.3	Unscheduled Maintenance	D	X	X	
161	3.1.9.3	Availability	A	X	X	C-C
162	3.1.9.3	Availability	A	X	X	C-C
163	3.1.10.1	General	T	T	X	
164	3.1.10.2	Radiation	A	X	X	C-I

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

165	3.1.10.2	Radiation	A	X	X	C-I
166	3.1.10.2	Radiation	A	X	X	C-I
167	3.1.10.2	Radiation	A	X	X	C-I
168	3.10.1.3	Electrical Safety	A	X	X	C-I
169	3.10.1.3	Electrical Safety	A	X	X	C-I
170	3.1.10.4	Ergonomic Safety	I	I	X	
171	3.1.10.4	Ergonomic Safety	I	I	X	
172	3.1.10.4	Ergonomic Safety	I	X	X	
173	3.1.10.5	Hazardous Materials	I	X	X	
174	3.1.10.5	Hazardous Materials	A	X	X	
175	3.1.10.5	Hazardous Materials	I	X	X	
176	3.1.11.1	Physical Security	I	I	X	
177	3.1.11.1	Physical Security	I	I	X	
178	3.1.11.2	Software Access	D	X	X	
179	3.1.11.2	Software Access	A	X	X	
180	3.1.11.2	Software Access	D	D	X	
181	3.1.11.2	Software Access	D	D	X	
182	3.1.11.3	Info. Tech. Security	A	X	X	
183	3.2.1.1.1.1	Explosives	A	X	X	Q-T
184	3.2.1.1.1.2	Weapons	A	X	X	Q-T
185	3.2.1.1.1.3	Liquids	A	X	X	Q-T
186	3.3.1.1.1.1	Explosives	A	X	X	Q-T
187	3.3.1.1.1.2	Weapons	A	X	X	Q-T

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

188	3.3.1.1.1.3	Liquids	A	X	X	Q-T
189	3.4.1	Automated Threat Detection Marking	D	X	X	
190	3.4.1	Automated Threat Detection Marking	D	X	X	
191	3.4.1	Automated Threat Detection Marking	D	X	X	
192	3.4.1	Automated Threat Detection Marking	D	X	X	
Appendix C						
193	n/a	User Access Levels and Capabilities	A	X	X	
Appendix D						
194	5.1	Baseline Voltage and Current Distortion	A	X	X	C-I
195	5.1	Baseline Voltage and Current Distortion	A	X	X	C-I
196	5.2	Power Usage Profile and Power Factor	A	X	X	C-I
197	5.3	Maximum Inrush Current Ration	A	X	X	C-I
198	5.4	Steady State Current Unbalance	A	X	X	C-I
199	5.4	Steady State Current Unbalance	A	X	X	C-I

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

200	5.4	Steady State Current Unbalance	A	X	X	C-I
201	5.4	Steady State Current Unbalance	A	X	X	C-I
202	5.5	Maximum Leakage Current	A	X	X	C-I
203	5.6	Voltage Sag and Interruption Withstand Performance	A	X	X	C-I
204	5.7	Uninterruptible Power Supply	A	X	X	C-I
Appendix E						
205	1.0	FDRS Report Display	D	X	X	
206	1.0	FDRS Report Display	D	X	X	
207	1.1	IO Log Report	D	X	X	
208	1.1	IO Log Report	D	X	X	
209	1.1	IO Log Report	D	X	X	
210	1.2	Event Report	D	X	X	
211	1.2	Event Report	D	X	X	
212	1.2	Event Report	D	X	X	
213	1.2	Event Report	D	X	X	
214	1.3	Access History	D	X	X	
215	1.3	Access History	D	X	X	

LEGEND 1

Verification Methods		Remarks
A	Analysis	See paragraph 4.2.1
D	Demonstration	See paragraph 4.2.2
I	Inspection	See paragraph 4.2.3
NV	Not verifiable	
T	Test	See paragraph 4.2.4
X	Not applicable	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

LEGEND 2

Certifications/Qualifications	
C-C	Certification by the Contractor
C-I	Certification by an independent evaluator (UL Listing or Equivalent is a certification performed by Underwriter's Laboratories or equivalent independent agency)
Q-T	Qualification by the Government (Transportation Security Laboratory)

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

5.0

ACRONYMS

AC	Alternating Current
A _i	Inherent Availability
ANSI	American National Standards Institute
BIT	Built-In Test
BRD	Business Rules Document
BS	Backscatter
C&A	Certification and Accreditation
CBEMA	Computer Business Manufacturers Association
CENELEC	European Committee for Electro-technical Standardization
CFR	Code of Federal Regulations
COTS	Commercial off the Shelf
DC	Direct Current
DHS	Department of Homeland Security
DISA	Defense Information Security Agency
DPF	Displaced Power Factor
DOT	Department of Transportation
EMC	Electromagnetic Compatibility
EN	European Standard
E-Stop	Emergency Stop
EUT	Equipment Under Test
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FDRS	Field Data Reporting System
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FIT	Fault Isolation Test
GED	General Equivalency Diploma
GUI	Graphical User Interface
Hi-SOC	High Speed Operational Connectivity
HSAR	Homeland Security Acquisition Regulation
HVAC	Heating, Ventilation, and Air Conditioning
ICNIRP	International Commission of Non-Ionizing Radiation Protection
ID	Identification
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IO	Image Operator
IOCP	Image Operator Control Panel
IP	Internet Protocol
IRD	Interface Requirements Document
ISSO	Information System Security Officer
IT	Information Technology
ITIC	Information Technology Industry Council
ITMRA	Information Technology Management Reform Act
ITSEC	IT Security

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

LRU	Line Replaceable Unit
MMW	Millimeter Wave
MSDS	Material Safety Data Sheet
MTBF	Mean Time Before Failure
MTBMA	Mean Time Between Maintenance Actions
MTTR	Mean Time To Repair
NEMA	National Electrical Manufacturers Association
NIST	National Institute of Standards and Technology
NRTL	National Recognized Test Laboratory
NSA	National Security Agency
OCP	Operator Control Panel
OS	Operating Security
OSHA	Occupational Safety and Health Administration
OTK	Operational Test Kit
Pd	Probability of Detection
PED	Personal Electronic Device
Pfa	False Alarm Rate
RF	Radio Frequency
RMS	Root Means Square
SO	Screening Operator
STD	Standard
STIP	Security Technology Integrated Program
TCP	Transmission Control Protocol
THD	Total Harmonic Distortion
TPF	Total Power Factor
TSA	Transportation Security Administration
TSE	Transportation Security Engineering
TSL	Transportation Security Laboratory
TSO	Transportation Security Officer
UL	Underwriters Laboratory
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VAC	Volts Alternating Current

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

**APPENDIX A: TRANSPORTATION SECURITY EQUIPMENT INFORMATION
TECHNOLOGY SECURITY REQUIREMENTS**

A.1 Scope

This document was created to identify specific requirements from the full set of information technology security requirements—found in TSA Management Directive 1400.3 and the DHS National Security Systems Handbook 4300.A—that are directly applicable to the hardware and software used for the Transportation Security Equipment (TSE) being designed and built and provides a reference of many of the findings that have been identified in past security test and evaluations of TSE.

A.2 References

The following documents were used in the development of this set of TSE Security Requirements:

DHS 4300 A	<i>Department of Homeland Security Sensitive Systems Handbook V3.2, October 1, 2005.</i>
DHS HP-UX Secure Baseline Configuration Guide	Department of Homeland Security HP-UX Secure Baseline Configuration Guide V2.1, May 31, 2007.
DHS Linux Secure Baseline Configuration Guide	Department of Homeland Security Linux Secure Baseline Configuration Guide V2.1, May 31, 2007.
DHS Solaris 10 Secure Baseline Configuration Guide	Department of Homeland Security Solaris 10 Secure Baseline Configuration Guide V1.1, May 31, 2007
DHS Windows 2003 Server Windows XP Windows Vista Secure Baseline Configuration Guide	Department of Homeland Security Windows 2003 Server Windows XP Windows Vista Secure Baseline Configuration Guide V1.1, May 31, 2007
FIPS 140-2	Security Requirements for Cryptographic Modules December 3, 2002 (Change Notice 2)
FIPS-180-3	Secure Hash Standard
FIPS-186	Digital Signature Standard.
FIPS-197	Advanced Encryption Standard.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

TSA MD 1400.3

Transportation Security Administration (TSA)
Management Directive No. 1400.3—TSA Information
Security Policy.

A.3 Operating System Security Requirements

A.3.1 Hardening Standards

The TSE shall have the Operating System (OS) software configured in compliance with the following OS Secure Baseline Configuration Guides:

- a. Linux-based operating systems to be configured in compliance with the DHS Linux Secure Baseline Configuration Guide V2.1 with exceptions as noted in section 3.1.1.1;
- b. Windows 2000 operating systems to be configured in compliance with the DHS Windows 2003-XP-Vista Secure Baseline Configuration Guide V2.1 with exceptions as noted in section 3.1.1.2;
- c. Windows XP operating systems to be configured in compliance with the DHS Windows 2003-XP-Vista Secure Baseline Configuration Guide V2.1 with exceptions as noted in section 4.1.1.2;
- d. Windows 2003 operating systems to be configured in compliance with the DHS Windows 2003-XP-Vista Secure Baseline Configuration Guide V2.1 with exceptions as noted in section 4.1.1.2;
- e. Windows Vista operating systems to be configured in compliance with the DHS Windows 2003-XP-Vista Secure Baseline Configuration Guide V2.1 with exceptions as noted in section 4.1.1.2;
- f. HP-UX operating systems to be configured in compliance with the DHS HP-UX Server Secure Baseline Configuration Guide V2.1;
- g. Solaris operating systems to be configured in compliance with the DHS Solaris Server Secure Baseline Configuration Guide V1.1; and
- h. For operating systems not listed above, the following sources to be consulted in the following order (i.e., if an OS guide is not available under source (1) then go to source (2)):
 1. National Security Agency (NSA) Security Configuration Guides available at http://www.nsa.gov/ia/guidance/security_configuration_guides/operating_systems.shtml;

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

2. Defense Information Security Agency (DISA) Security Technical Implementation Guides at <http://iase.disa.mil/stigs/stig/index.html>; and
3. National Institute of Standards and Technology (NIST) Configuration Checklist Program at <http://checklists.nist.gov/>

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

A.3.2 Hardening Standards Specifics

A.3.2.1 Deviations from DHS Linux Secure Baseline Configuration Guide V2.1

The following deviations to the DHS Linux Secure Baseline Configuration Guide shall be followed:

- a. The TSE OS to be hardened to the "Enterprise Server" setting;
- b. The TSE OS to be hardened using the configurations in Appendix A of the DHS Linux Server Secure Baseline V2.1;
- c. Sections 1.2 and 1.6 Root and other interactive accounts on TSE to have passwords that do not expire;
- d. Section 2.9 X11 Forwarding not configured in sshd.conf;
- e. Section 3.1 TSE to be configured to use a local syslog file in lieu of a remote syslog server;
- f. Section 5.5 TSE to be configured in /etc/inittab to disable a ctrl-alt-delete key combination;
- g. Section 6.1 Bastille Linux settings not applied; and
- h. Section 6.4 USB to remain operational.

A.3.2.2 Deviations from DHS Windows 2003-XP-Vista Secure Baseline Configuration Guide V2.1

The following deviations to the DHS Windows 2003-XP-Vista Secure Baseline shall be followed:

- a. The TSE OS to be hardened to the "XP" setting for Windows XP operating systems;
- b. The TSE OS to be hardened to the "Vista" setting for Windows Vista operating systems;
- c. The TSE OS to be hardened to the "SOHO" setting for Windows 2000, 2003, and 2008 operating systems;
- d. Section 1 Admin and other OS interactive accounts on TSE to have passwords that do not expire;

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

- e. Section 10 Windows Update not configured for automatic update;
- f. Section 10 The TSE implements Symantec Antivirus V10 software that is configured to check all files; and
- g. Section 10 The TSE implements Symantec Antivirus V10 software that is configured for automatic updates from the TSA Symantec Enterprise Manager.

A.3.3 Patching

The TSE operating system baseline shall:

- a. Be of a version that is currently supported by the operating system Contractor; and
- b. Not be of a version that has been announced as End-of-Life by the operating system Contractor.

A.3.4 Wireless

The TSE shall not have any of the following wireless technologies detectable from a distance of 10 feet or more away from the TSE:

- a. IEEE 802.11a Wi-Fi;
- b. IEEE 802.11b Wi-Fi;
- c. IEEE 802.11g Wi-Fi;
- d. IEEE 802.11n Wi-Fi;
- e. IEEE 802.16e Wi-Max; and
- f. IEEE 802.15 Bluetooth.

A.4 Application Security Requirements

This section contains requirements applicable to the applications used by TSE operators.

A.4.1 Access Control

The TSE User Application shall:

- a. Force users to make Personal Identification Numbers (PINs) that:
 - 1. Are a minimum of eight (8) characters and a maximum of 15 character in length;
 - 2. Are not be the same as the User ID;
 - 3. Cannot be reused for a minimum of 6 change cycles;
 - 4. Are changed every 90 days;
 - 5. Are numeric only;
 - 6. Do not contain any two identical consecutive characters (example: 14588904); and

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

7. Contain no more than three identical consecutive characters in any position from the previous PIN.
- b. Authenticate the user via PIN each time the user logs into the system;
- c. Upon successful logon, notify the user of the following items:
 1. date and time of the last successful logon using this user identity; and
 2. The number of unsuccessful logon attempts using this user identity since the last successful logon.
- d. Force logoff of the user after a configurable amount of time of inactivity:
 1. Forced user logoff which is configurable in 1-minute increments;
 2. Forced user logoff which has a minimum of 0 minutes; and
 3. Forced user logoff which has a maximum of 90 minutes.
- e. Allow only one logon per user id at a time; and
- f. Upon successful logon, display the DHS-approved warning banner as stated in DHS 4300A, paragraph 5.2.3:

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use or access of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following: You have no reasonable expectation of privacy when you use this information system; this includes any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may, without notice, monitor, intercept, search and seize any communication or data transiting or stored on this information system.

The government may disclose or use any communications or data transiting or stored on this information system for any lawful government purpose, including but not limited to law enforcement purposes.

You are NOT authorized to process classified information on this information system.

A.4.2 Audit and Accountability

The TSE User Application shall:

- a. Automatically log the following events:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

1. Application software startup and shutdown;
 2. Successful and unsuccessful logons;
 3. User PIN changes;
 4. Data export and import to and from removable media; and Software configuration changes;
- b. Encrypt or hash user PINs when stored in logs; and
- c. Make available Log events, as described in the Field Data Reporting System Table below:

Output Field	Description	Format
Login ID	Unique Logon ID of the user	Numeric
Process Name	Software application	
Event Date	Date event occurred	mm-dd-yyyy
Event Time	Time event occurred	hh:mm:ss
Attempted Action	Description of the action that was attempted	At a minimum, possible choices include: Application startup; Application shutdown; User logon; Enter maintenance mode; Exit maintenance mode; User PIN change; Data export to removable media; Import from removable media; Software configuration change.
Event Outcome	Outcome of the logged event	Use S for Success F for Fail

A.5 Requirements for Networked Transportation Security Equipment

This section is only applicable to TSE that are to be connected to the TSA's Network. For example, TSE selected to be integrated into the STIP program. Network traffic requirements only apply to traffic across the TSA's network and not internal to multicomponent TSEs.

A.5.1 Operating System Firewall

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

The TSE shall use a software firewall with a "default deny" policy for interfaces connected to the TSA's network.

A.5.1.1 Secure Start-Up Configuration

During bootup of the TSE, the firewall policies shall be applied immediately after the network connection has an internet protocol address.

A.5.1.2 Allowable Traffic

The TSE firewall shall allow only the following bidirectional traffic across TSA's network:

- a. UDP port 53 to TSA domain nameservers;
- b. TCP port 443 only to the TSA STIP servers;
- c. UDP port 123 to the TSA NTP servers;
- d. TCP ports 2967 and 2968 to the TSA anti-virus servers;
- e. ICMP types 0, 3, 4, 5, 8, and 11; and
- f. UDP ports 67 and 68 for Dynamic Host Control Protocol (DHCP).

A.5.2 Network Connections

A.5.2.1 Network Protocols

The TSE:

Shall not use the following unencrypted network protocols across the TSA's network:

1. File Transfer Protocol (FTP), and
 2. Telnet, and
- a. Shall use Secure Shell, Secure Sockets Layering, or Transport Layer Security in lieu of unencrypted network protocols.

A.5.2.2 Virtual Private Network

TSE shall not use Virtual Private Networking.

A.5.2.3 Remote Access

TSE shall not be configured for the following types of remote access across the TSA's network:

- a. Remote Desktop Protocol,
- b. Virtual Network Computing,
- c. Secure Shell, and

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

d. X11 Windowing System.

A.6 Encryption

TSE cryptographic modules shall be in compliance with the current versions of the following standards:

- a. Software modules validated under FIPS 140-2 to level 1;
- b. Hardware modules validated under FIPS 140-2 to level 2;
- c. Hash implementations compliant with FIPS 180; and
- d. Digital signature implementations compliant with FIPS 186-3.

A.7 Verification Requirements Traceability Matrix

The Verification Requirements Traceability Matrix (VRTM) shown in Table 1, defines the verification method to be used to validate each security requirement.

Table B-1: Verification Requirements Traceability Matrix

Req.	Para. #	Para. Title	FAT&E	Remarks
	3.0	Operating System Security Requirements	X	
	3.1	OS Hardening	I	
	3.1(a)	OS Hardening	I	
	3.1(b)	OS Hardening	I	
	3.1(c)	OS Hardening	I	
	3.1(d)	OS Hardening	I	
	3.1(e)	OS Hardening	I	
	3.1(f)	OS Hardening	I	
	3.1(g)	OS Hardening	I	
	3.1(h)	OS Hardening	X	
	3.1(h)(1)	OS Hardening	I	
	3.1(h)(2)	OS Hardening	I	
	3.1(h)(3)	OS Hardening	I	
	3.1.1	Hardening System Specifics	X	
	3.1.1.1	Deviations from DHS Linux Secure Baseline Configuration Guide V2.1	I	
	3.1.1.1(a)	Deviations from DHS Linux Secure Baseline Configuration Guide V2.1	I	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

Req.	Para. #	Para. Title	FAT&E	Remarks
	3.1.1.1(b)	Deviations from DHS Linux Secure Baseline Configuration Guide V2.1	I	
	3.1.1.1(c)	Deviations from DHS Linux Secure Baseline Configuration Guide V2.1	I	
	3.1.1.1(d)	Deviations from DHS Linux Secure Baseline Configuration Guide V2.1	I	Shall Not
	3.1.1.1(e)	Deviations from DHS Linux Secure Baseline Configuration Guide V2.1	I	
	3.1.1.1(f)	Deviations from DHS Linux Secure Baseline Configuration Guide V2.1	I	
	3.1.1.1(g)	Deviations from DHS Linux Secure Baseline Configuration Guide V2.1	NV	Shall Not
	3.1.1.1(h)	Deviations from DHS Linux Secure Baseline Configuration Guide V2.1	T	
	3.1.1.2	Deviations from DHS Windows 2003-XP-Vista Secure Baseline Configuration Guide V2.1	I	
	3.1.1.2(a)	Deviations from DHS Windows 2003-XP-Vista Secure Baseline Configuration Guide V2.1	I	
	3.1.1.2(b)	Deviations from DHS Windows 2003-XP-Vista Secure Baseline Configuration Guide V2.1	I	
	3.1.1.2(c)	Deviations from DHS Windows 2003-XP-Vista Secure Baseline Configuration Guide V2.1	I	
	3.1.1.2(d)	Deviations from DHS Windows 2003-XP-Vista Secure Baseline Configuration Guide V2.1	I	
	3.1.1.2(e)	Deviations from DHS Windows 2003-XP-Vista Secure Baseline Configuration Guide V2.1	I	Shall Not
	3.1.1.2(f)	Deviations from DHS Windows 2003-XP-Vista Secure Baseline Configuration Guide V2.1	I	
	3.1.1.2(g)	Deviations from DHS Windows 2003-XP-Vista Secure Baseline Configuration	I	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

Req.	Para. #	Para. Title	FAT&E	Remarks
		Guide V2.1		
	3.2	Patching	X	
	3.2(a)	Patching	I,A	
	3.2(b)	Patching	I,A	Shall Not
	3.3	Wireless	X	
	3.3(a)	Wireless	T	Shall Not
	3.3(b)	Wireless	T	Shall Not
	3.3(c)	Wireless	T	Shall Not
	3.3(d)	Wireless	T	Shall Not
	3.3(e)	Wireless	T	Shall Not
	3.3(f)	Wireless	T	Shall Not
	4.0	Application Security Requirements	X	
	4.1	Access Control	X	
	4.1(a)	Access Control	D	
	4.1(a)(1)	Access Control	D	
	4.1(a)(2)	Access Control	D	Shall Not
	4.1(a)(3)	Access Control	D	Shall Not
	4.1(a)(4)	Access Control	D	
	4.1(a)(5)	Access Control	D	
	4.1(a)(6)	Access Control	D	Shall Not
	4.1(a)(7)	Access Control	D	Shall Not
	4.1(b)	Access Control	D	
	4.1(c)	Access Control	X	
	4.1(c)(1)	Access Control	D	
	4.1(c)(2)	Access Control	D	
	4.1(d)	Access Control	X	
	4.1(d)(1)	Access Control	I	
	4.1(d)(2)	Access Control	I	
	4.1(d)(3)	Access Control	I	
	4.1(e)	Access Control	D	
	4.1(f)	Access Control	D	
	4.2	Audit and Accountability	X	
	4.2(a)	Audit and Accountability	X	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

Req.	Para. #	Para. Title	FAT&E	Remarks
	4.2(a)(1)	Audit and Accountability	D	
	4.2(a)(2)	Audit and Accountability	D	
	4.2(a)(3)	Audit and Accountability	D	
	4.2(a)(4)	Audit and Accountability	D	
	4.2(a)(5)	Audit and Accountability	D	
	4.2(b)	Audit and Accountability	I	
	4.2(c)	Audit and Accountability	I	
	5.0	Requirements for Networked Transportation Security Equipment	X	
	5.1	Operating System Firewall	I	
	5.1.1	Secure Startup Configuration	I	
	5.1.2	Allowable Traffic	X	
	5.1.2(a)	Allowable Traffic	I,T	
	5.1.2(b)	Allowable Traffic	I,T	
	5.1.2(c)	Allowable Traffic	I,T	
	5.1.2(d)	Allowable Traffic	I,T	
	5.1.2(e)	Allowable Traffic	I,T	
	5.1.2(f)	Allowable Traffic	I,T	
	5.2	Network Connections	X	
	5.2.1	Network Protocols	X	
	5.2.1(a)	Network Protocols	I,T,A	Shall Not
	5.2.1(a)(1)	Network Protocols	I,T,A	Shall Not
	5.2.1(a)(2)	Network Protocols	I,T,A	Shall Not
	5.2.1(b)	Network Protocols	I,T,A	
	5.2.2	Virtual Private Networking	I,T,A	Shall Not
	5.2.3	Remote Access	X	Shall Not
	5.2.3(a)	Remote Access	I,T	Shall Not
	5.2.3(b)	Remote Access	I,T	Shall Not
	5.2.3(c)	Remote Access	I,T	Shall Not
	5.2.3(d)	Remote Access	I,T	Shall Not
	5.3	Encryption	X	
	5.3(a)	Encryption	C-I	
	5.3(b)	Encryption	C-I	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

Req.	Para. #	Para. Title	FAT&E	Remarks
	5.3(c)	Encryption	C-I	
	5.3(d)	Encryption	C-I	
	3.0	Operating System Security Requirements	X	
	3.1	OS Hardening	I	
	3.1(a)	OS Hardening	I	
	3.1(b)	OS Hardening	I	
	3.1(c)	OS Hardening	I	
	3.1(d)	OS Hardening	I	
	3.1(e)	OS Hardening	I	
	3.1(f)	OS Hardening	I	
	3.1(g)	OS Hardening	I	

LEGEND

Acronym	Test
DT&E	Developmental Test and Evaluation
FAT	Factory Acceptance Test

Verification Methods	
A	Analysis
D	Demonstration
I	Inspection
NV	Not verifiable
T	Test
X	Not applicable

Certifications	
C-C	Certification by the Contractor
C-I	Certification by an independent evaluator (UL Listing or Equivalent is a certification performed by Underwriter's Laboratories or equivalent independent agency)
C-T	Certification by the Transportation Security Laboratory (TSL)

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

APPENDIX B FIELD DATA REPORTING SYSTEM REQUIREMENTS

DATA ELEMENTS

The data elements to be collected by the AIT system are described in the following five tables:

Table	Title	Content
I	Operator Log Information	Information for each IO Session.
II	System Event Information	Information for each system event
III	Access History Information	Information for data and report access
IV	Scan Information	Information for each scan completed by the AIT System.
V	User Data File	User Data Information

TABLE I. Operator Log Information.

Field Name	Field Description	Field Format	Field Values/Comments
MACHINE_ID	Identification number of the AIT system	String (length = 8)	Upon contract award a Contractor identifier will be assigned by the Government. The field format is a total length of eight (Contractor identifier plus AIT System serial number).
User_ID	Identification login of the IO	String (length = 15)	
FirstName	IO First Name	String (length = 30)	
LastName	IO Last Name	String (length = 30)	
LoginTime	IO Login Time	String (length = 19)	mm-dd-yyyy_hh:mm:ss
LogoutTime	IO Logout Time	String (length = 19)	mm-dd-yyyy_hh:mm:ss
PaxCount	Number of passengers scanned	Integer	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

Field Name	Field Description	Field Format	Field Values/Comments
	during session		
PaxSuspectCount	Number of passengers suspect during session	Integer	
PaxClearCount	Number of passengers cleared during session	Integer	
Affiliation	Company the IO works for (TSA or Contractor)	String (length = 50)	
SiteCode	FAA Airport Code	String (length = 3)	Such as: SNA, BOS, EWR
SubsiteCode	Machine Location	String (length = 20)	Example: "Terminal 1 Lane 2"
ITModelNo	Model Number of the AIT System	String (length = 8)	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

TABLE II. System Event Information.

Field Name	Field Description	Field Format	Field Values/Comments
MACHINE_ID	Identification number of the AIT System	String (length = 8)	Upon contract award a Contractor identifier will be assigned by the Government. The field format is a total length of eight (Contractor identifier plus serial number).
ITModelNo	Model Number of the AIT System	String (length = 8)	
SiteCode	FAA Airport Code	String (length = 3)	Such as: SNA, BOS, EWR
SubsiteCode	Machine Location	String (length = 20)	Example: "Terminal 1 Lane 2"
SoftVers	AIT system software version identification	String (length = 30)	Contractor assigned software version identification for the software running on the AIT System
User_ID	Identification login of the IO	String (length = 15)	
FirstName	IO Name	String (length = 30)	
LastName	IO Name	String (length = 30)	
AccessLevel	Access Control Level	String (length = 1)	
Affiliation	IO Affiliation	String (length = 15)	
Event_Time	At what time did the event occurred?	String (length = 19)	mm-dd-yyyy_hh:mm:ss
Event	What event occurred?	String (length = 25)	At a minimum, possible choices include: account creations, modify account, machine fault resets, IO logoff, IO logon, Operational mode change. View reports, download data, software restart, system errors, system startup,

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

Field Name	Field Description	Field Format	Field Values/Comments
			system shutdown.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

TABLE III. Access History Information.

Field Name	Field Description	Field Format	Field Values/Comments
MACHINE_ID	Identification number of the AIT SYSTEM	String (length = 8)	Upon contract award a Contractor identifier will be assigned by the Government. The field format is a total length of eight (Contractor identifier plus serial number).
User_ID	Identification login of the IO	String (length = 15)	
AccessLevel	Access Control Level	String (length = 1)	
Action	System action	Integer	Use 1=download files 2=change parameters 3=enter/modify users 4=view reports
ActionTime	Time action occurred	String (length = 19)	mm-dd-yyyy_hh:mm:ss
ReportType	Report type	Integer	Use 1=IO Log Report 2=Event Log Report 3=Access History Report
Downloaded	Was the file downloaded?	String (length=1)	Use D=Downloaded N=Not Downloaded

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

TABLE IV. Scan Information.

Field Name	Field Description	Field Format	Field Values/Comments
MACHINE_ID	Identification number of the AIT system	String (length = 8)	Upon contract award a Contractor identifier will be assigned by the Government. The field format is a total length of eight (Contractor identifier plus AIT System serial number).
SoftVers	AIT system software version identification	String (length = 30)	Contractor assigned software version identification for the software running on the AIT System
ImageStart	Date and time the passenger scan starts	String (length = 19)	mm-dd-yyyy_hh:mm:ss
ImageComplete	Date and time the passenger scan completes	String (length = 19)	mm-dd-yyyy_hh:mm:ss
IORespTime	Date and time the IO decision is made	String (length = 19)	mm-dd-yyyy_hh:mm:ss
IO Decision	Nature of IO response	String (length = 1)	Use C for Clear S for Suspect
User_ID	Identification login of the IO	String (length = 15)	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

TABLE V. User Data File.

Field Name	Field Description	Field Format	Field Values/Comments
FirstName	TSO Name	String (length = 30)	
LastName	TSO Name	String (length = 30)	
User_ID	Identification login of the TSO	String (length = 15)	
Password	TSO Password	String (length = 15)	
Affiliation	TSO Affiliation	String (length = 15)	
AccessLevel	Access Control Level	String (length = 1)	
Status	User Status	String (length = 1)	Use 1=active 0=inactive
StatusDate	Date current status was activated	String (length = 19)	mm-dd-yyyy_hh:mm:ss

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

APPENDIX C USER ACCESS LEVELS AND CAPABILITIES

User access and associated capabilities, based on username, password, and user access level, *shall* (193) be as outlined in the Access Control Levels Table.

Access Control Levels Table

User Access Level	User	Capabilities
Z	Transportation Security Administration Headquarters Contractor Maintenance Technician (see Note 1) Super User	Logon and Logoff Startup and Shutdown Enable/Disable Image Filters Access Test Mode Export Raw Image Data in Test Mode Upload/Download User Database Create and Modify Accounts (All Users) Download Data (see Note 1) Set and Alter Passwords (All Users) (see Note 1) Modify Baselined or Fielded Software (see Note 1) Access Operating System <u>Note 1:</u> Contractor Maintenance Technicians shall not set or alter passwords and shall download data only without alteration. Contractor "superuser" passwords will be disabled by a Government representative after site acceptance. Only Government approved software changes shall be made to the baselined or fielded software.
1	Federal Security Director Screening Manager Screening Supervisor	All Access Level 2 Capabilities Logon and Logoff Startup and Shutdown Enable/Disable Auto-Detect Highlighting Create/Modify Accounts (Level 2)
2	Lead-In-Charge	All Access Level 3 Capabilities Perform Daily Preventative Maintenance Create and Modify Accounts (Level 3) Access and view AIT system FDRS Database and Reports Access and view AIT system User Database Download AIT system FDRS Data Calibrate system

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

User Access Level	User	Capabilities
3	Operators	Logon and Logoff Startup and Shutdown Access Screening Mode Screens Passengers Initiate Fault Isolation Test

~~**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

APPENDIX D TSA OPERATIONAL POWER REQUIREMENTS

1.0 INTRODUCTION

The purpose of this document is to define the minimum power performance requirements for any detection system that identifies potential threats on a person, an article of baggage, a parcel or cargo. The standards, on which these requirements were based, have been adopted from the FAA Specification Document: *Electronic Equipment, General Requirements* (FAA-G-2100H).

2.0 OVERVIEW

The requirements defined in this document were generated from the results of eight different electronic screening device tests, from the point-of-view of "power system performance." The tests were conducted between August 21st and August 25th 2006, at the Transportation Security Laboratory (TSL) and the Doughty Road Laboratory. The objective of these tests was to provide confidence, as well as validate the compatibility of TSA's equipment with the available electrical supply at its various deployment locations. Special attention was given to the equipment's power profile, energy consumption, and vulnerability to power system events (i.e., voltage sags and drops). Each system was tested to define the baseline electrical performance relative to:

- (a) The respective equipment data sheets,
- (b) The current Commercial-Off-the-Shelf (COTS) procurement specification, and
- (c) The actual system voltage sag and interruption withstand performance.

The recorded results of these tests are expected to provide procurement and specification personnel with a better understanding of the impact that detection systems have on other facility equipment, in addition to their internal components. This includes the sensitivities of detection systems to some of the more common power quality variations that may be encountered at locations where the detection systems are deployed.

3.0 EQUIPMENT

For the purpose of this document, "detection systems" will refer to all screening devices using bulk, trace, or any other technology to screen passengers and their luggage before entering a secure area (e.g., Checked Baggage Systems, Checkpoint Systems, Cargo Screening Systems, or any other passenger and baggage screening system).

4.0 MEASUREMENT

Power over an entire operational cycle tends to vary as heaters, compressors, and other cyclic loads turn on and off. The measured "Maximum Steady State Load" will identify the highest level of power drawn consistently over a measured period of time (e.g., 4 kW for 5 min, with no changes). Therefore, the Maximum Steady State Load must be maintained during a full operational cycle while power requirements are measured and recorded.

5.0 POWER PERFORMANCE DATA ACQUISITION AND REQUIREMENTS ANALYSIS

5.1 Baseline Voltage and Current Distortion

The baseline voltage and current distortion measurement identifies the harmonic current distortion of the equipment and determines how that current distortion level will distort the voltage at the supply point.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Total Harmonic Distortion – The “Total Harmonic Distortion” will be calculated as the square root of the cumulative sum of each measured distortion over several operational cycles.

The **maximum** Total Harmonic Distortion (THD) during a full operational cycle for detection systems *shall* (194) be less than three percent (<3%), as specified in the following references:

- (a) IEEE 519, Harmonic Limits and
- (b) FAA-G-2100H, 3.1.1.3.2.f, Inrush Current.

Individual Harmonic Distortion – The measured “Individual Harmonic Distortion” will identify the maximum distortion of the equipment during any operational cycles over a specific period of time.

The maximum Individual Harmonics (I_N) during any given cycle for detection systems *shall* (195) be less than three percent (<3%), as specified in the following references:

- (a) IEEE 519, Harmonic Limits and
- (b) FAA-G-2100H, 3.1.1.5.c, Table 1, Harmonics.

5.2 Power Usage Profile and Power Factor

The power usage profile and power factor measurement evaluates the minimum and maximum power drawn during a full operational cycle of the equipment. Once the full load power draw is determined, the power factor is measured at the full load value.

Power Factor (at maximum steady state loading) – Standard measure of “Power Factor” includes two methods, Displaced Power Factor (DPF) and Distortion Power Factor, or Total Power Factor (TPF). As long as the meter being used integrates the instantaneous voltage and currents over each cycle of the power frequency, the calculated Power Factor will be accurate regardless of the method selected.

The Power Factor at maximum steady state loading *shall* (196) be greater than point six (> .6) for all detection systems, as specified in the following reference:

- (a) FAA-G-2100H, 3.1.1.3.1, Power Factor.

5.3 Maximum Inrush Current Ratio

The inrush current measurement assesses the maximum peak inrush of the equipment during a full operational cycle and determines how that peak inrush compares to the maximum steady state Root Means Square (RMS) current drawn.

Max Inrush Current Ratio – The maximum inrush current ratio will compare both the Maximum Peak Inrush ($I_{\max \text{ peak}}$) and the maximum steady state RMS current ($I_{\max \text{ RMS}}$) through the following formula:

$$I_{\max \text{ peak}} / I_{\max \text{ RMS}}$$

The **maximum** “Inrush Current Ratio” during a full operational cycle for detection systems *shall* (197) be less than twenty times (< 20) the steady state, as specified in the following references:

- (a) IEC/EN61000-3-3, Flicker and Voltage Variation and
- (b) FAA-G-2100H, 3.1.1.3.2.h, Inrush Current.

5.4 Steady State Current Unbalance

The steady state current unbalance measures the current unbalance of the equipment and determines how that current unbalance value compares to the COTS procurement specification.

Avg. Current Unbalance ($I_{UNB\text{ Avg}}$) – The average current unbalance will be the sum of each current unbalance measured over the course of several operational cycles.

- (a) The **average** current unbalance measured for detection systems *shall* (198) be less than ten percent (< 10 %), as specified in the following references:
 - i. National Electrical Manufacturers Association (NEMA) – M61 and
 - ii. FAA-G-2100H, 3.1.1.4., Electric Load Balance.
- (b) The **average** current unbalance measured for detection systems *shall* (199) be verified and adjusted as needed during site acceptance.

Max Current Unbalance ($I_{UNB\text{ Max}}$) – A three-phase system is called balanced if the three-phase voltages and currents have the same amplitude and are phase shifted by 120° with respect to each other. If either or both of these conditions are not met, the system is considered unbalanced or asymmetrical. Thus the maximum current unbalance is the maximum current measured that is out of symmetry, with respect to the other phases. (Note: Under multiple system configurations, it is possible for the current unbalance of one system to be neutralized by the current unbalance of the next system (based on phase and direction)).

- (a) The **maximum** current unbalance for threat detection systems *shall* (200) be identified for each system to substantiate the calculation, sizing and integration of multiple configurations of the same equipment.
- (b) The **maximum** current unbalance for threat detection systems *shall* (201) be verified and adjusted as needed during site acceptance.

5.5 Maximum Leakage Current

The intent of the maximum leakage current measurement is to identify the maximum leakage current injected onto the ground conductor by the equipment, during a full operational cycle. In addition, this measurement will help determine how that value might need to be correlated to ground fault protection settings, if applicable at the installation location.

Maximum Leakage Current – The maximum leakage current is the current that flows from the unit through the grounding conductor into a facility ground. Leakage current could shock an individual if the household grounding is not sufficient or there is an intentional or unintentional interruption of grounding connection.

- (a) The **maximum** leakage current measured for detection systems *shall* (202) be less than or equal to three and a half milliamps (3.5mA) as specified in the following references:
 - i. UL Standard 60950, clause 5.1.7,
 - ii. IEC 60601-1, General requirements for basic safety and essential performance, and
 - iii. IEEE Transactions on Very large Scale Integration (VLSI) Systems, 12(2):131-139.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

5.6 Voltage Sag and Interruption Withstand Performance

The voltage sag and interruption withstand measurement evaluates the capability of the equipment to withstand power faults which result in momentary power system interruptions. The secondary objective of this requirement is to evaluate the system drop-off and subsequent restart time.

Voltage Sag – The voltage sag measurement identifies the length of time and percentage below nominal usage that a system can tolerate, if the power source is interrupted or eliminated during normal operations.

- (a) The voltage sag for detection systems *shall* (203) tolerate a zero voltage for a minimum duration of twenty milliseconds (20 ms) as specified in the following references:
 - i. IEC 61000-4-34, Voltage Sag Immunity,
 - ii. IEC 61000-4-11, Voltage Dip Immunity, and
 - iii. ITIC (CBEMA) Curve 07.01.2000.

5.7 Uninterruptible Power Supply

The presence of an Uninterruptible Power Supply (UPS) demonstrates the systems ability to shield against unexpected power fluctuations, voltage sags or temporary power losses from the power distribution sources. As a byproduct of power performance, a weak UPS can cause unwarranted system reboots, hang-ups, and several other system anomalies.

Uninterruptible Power Supply – The health of a UPS can be significantly affected by the system's ability to tolerate the variance of power over short periods of time. Measuring the strength of the UPS identifies the systems ability to maintain operational availability during moments of critical power failure.

The UPS, if present, *shall* (204) be configured into the core system for automated monitoring and display of the current health and condition of the UPS.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

APPENDIX E AIT REPORTS

1.0 FDRS REPORT DISPLAY

The AIT system *shall* (205) provide the reports listed in Table 1 below. Data reports (Reports 1, 2 and 3) *shall* (206) be viewable by calendar month and year (e.g., February 2008).

Table 1. AIT Data Reports

Report	Report Name
1	IO Log Report
2	Event Report
3	Access History Report

1.1 IO LOG REPORT

The IO Log Report *shall* (207) present an overview of all IOs who worked each day for the selected month, along with their locations and login/logout times. The IO Summary Report *shall* (208) contain one record / row in the output table for each login session occurring in the date range. This report *shall* (209) be downloadable and be viewable on the IO Station monitor.

Output Field	Description	Format
User_ID	Identification login of the IO	String (length = 15)
LastName	IO Last Name	String (length = 15)
FirstName	IO First Name	String (length = 15)
LoginTime	IO Login Timestamp	String (length = 19)
LogoutTime	IO Logout Timestamp	String (length = 19)
PaxCount	Number of passengers scanned during session	Integer
PaxSuspectCount	Number of passengers suspected during session	Integer
PaxClearCount	Number of passengers cleared during session	Integer
Affiliation	IO Affiliation	String (length = 15)
ITModelNo	Model Number of the AIT System	String (length = 8)

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

Output Field	Description	Format
SiteCode	FAA Airport Code	String (length = 3)
SubsiteCode	Machine Location	String (length = 20)

1.2 EVENT REPORT

An Event Report containing details of each system event *shall* (210) be provided. This report *shall* (211) consist of one row per event, and *shall* (212) provide data indicated in the following table. This report *shall* (213) be downloadable and be viewable on the IO Station monitor.

Output Field	Description	Format
MACHINE_ID	Identification Number of the AIT System	String (length = 8)
LastName	IO Last Name	String (length = 15)
FirstName	IO First Name	String (length = 15)
User_ID	Identification login of the IO	String (length = 15)
SiteCode	FAA Airport Code	String (length = 3)
Event_Time	Time event occurred	String (length = 19)
Event	Description of event	String (length = 25)

1.3 ACCESS HISTORY REPORT

The Access History Report *shall* (214) report who modified system settings as well as the time and nature of the modification using the format described below. The Access History report also presents detail on administrative operations activity (i.e., who accessed the report, the type of report, and when the report was accessed). This report *shall* (215) be downloadable and be viewable on the IO Station monitor.

Output Field	Description	Format
MACHINE_ID	Identification Number of the AIT System	String (length = 8)
User_ID	Identification login of the IO	String (length = 15)
AccessLevel	Access Control Level	String (length = 1)

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

OST-ENG-AIT-PROCSPEC-2.1

09/10/09

Output Field	Description	Format
Action	System action	Integer
ActionTime	Time action occurred	String (length = 19)
ReportType	Report type	Integer
Downloaded	Was the file downloaded?	String (length=1)

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.