TRANSPORTATION SECURITY ADMINISTRATION

OFFICE OF SECURITY TECHNOLOGY
SYSTEM PLANNING AND EVALUATION

PROCUREMENT SPECIFICATION FOR
WHOLE BODY IMAGER DEVICES FOR CHECKPOINT OPERATIONS

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

23 September 2008
FINAL, Version 1.02

U.S. Department of Homeland Security
Transportation Security Administration

Prepared By:
TSA Office of Security Technology

Technical Report Documentation Page		
1. Report No. DHS/TSA/OST/ENG/WBI-001	**2. Government Accession No.** N/A	**3. Recipient's Catalog No.** N/A
4. Title and Subtitle Procurement Specification for Whole Body Imager Devices for Checkpoint Operations		**5. Report Date** 23 September 2008 **6. Performing Organization Code** TSA-16
7. Author Office of Security Technology System Planning and Evaluation Group		**8. Performing Organization Report No.** DHS/TSA/OST/ENG/WBI-001
9. Performing Organization Name and Address Transportation Security Administration Office of Security Technology System Planning and Evaluation 601 South 12th 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 Whole Body Imager hereinafter referred to as the WBI. Whole Body Imaging (WBI) 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** 70 / **22. Price**
Reproduction of completed page authorized		

DOCUMENT CHANGE HISTORY

b6 [redacted]

Version	Description – Author	Date
0.01	Initial Draf [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 Upda [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 [redacted]	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

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.

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 BACKGROUND

The Department of Homeland Security (DHS), Transportation Security Administration (TSA), presents the Whole Body Imager (WBI) 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 the WBI systems.

1.3 SYSTEM DESCRIPTION

WBI 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 WBI 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

WBI 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 WBI 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 WBI screening process.
Shall	Bolded, italicized "shalls" are requirements that the vendors' submitted WBI 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 WBI either locally or remotely.
WBI System	The combined performance of the WBI including the operator in the loop.

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 Security Technology Integrated Program (STIP) Business Rules Document (BRD), 13 August 2007
	TSA Security Technology Integrated Program (STIP) Transportation Security Equipment (TSE), Interface Requirements Document (IRD), Version 3.11, 14 April 2008
	TSA WBI Classified Detection Appendix, Version 2.0, September 23, 2008

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
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
UL 61010A-1	Electrical Equipment for Laboratory Use; Part 1: General Requirements, 30 January 2002
	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.

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

b2 b3

3.1.1.1.1.1 Explosives

The WBI System ***shall*** (2) produce images to enable an operator to determine the presence and location of explosives [redacted]

4(i)

3.1.1.1.1.2 Weapons

The WBI System ***shall*** (3) produce images to enable an operator to determine the presence and location of weapons [redacted]

3.1.1.1.1.3 Liquids

The WBI System ***shall*** (4) produce images to enable an operator to determine the presence and location of liquids [redacted]

3.1.1.1.1.4 Other Anomalies

The WBI System ***shall*** (5) produce images to enable an operator to determine the presence and location of other anomalies [redacted]

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, WBI 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 WBI will provide two distinct modes of operation: Screening Mode and Test Mode as defined in 3.1.1.3.1.

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

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

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

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

The WBI ***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 WBI ***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 WBI ***shall*** (15) be able to scan passengers with a height of up to at least 195 cm. Passenger access to the WBI imaging area ***shall*** (16) be no less than 85 cm wide. The WBI ***shall*** (17) require passengers to be no less than 8 cm and no more than 120 cm from the system in order to complete a scan.

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

3.1.1.3.1.1.1 Multiplexing

The WBI system ***shall*** (21) provide a means to multiplex images, allowing up to 64 IOCPs to receive images from up to 64 WBI systems utilizing the network requirements set forth in section 3.1.1.3.6.

3.1.1.3.1.2 Test Mode

For purposes of testing, evaluation, and training development, the WBI ***shall*** (22) provide a Test Mode. The WBI Test Mode ***shall*** (23) be the sole mode of operation permitting the exporting of image data. WBI Test Mode ***shall*** (24) be accessible as provided in the User Access Levels and Capabilities appendix.

When in Test Mode, the WBI:

- ***shall*** (25) allow exporting of image data in real-time;
- ***shall*** (26) prohibit projection of an image to the IO station;
- ***shall*** (27) provide a secure means for high-speed transfer of image data;
- ***shall*** (28) allow exporting of image data (raw and reconstructed).

3.1.1.3.2 Start-Up and Power-Down

The WBI SO station ***shall*** (29) have start-up and power-down procedures or functions at the Screening Operator Station (see Section 3.1.1.4.1 below) that ***shall*** (30), upon completion of start-up, display a login window.

The WBI IO station ***shall*** (31) display a login window upon completion of SO Station start-up.

The WBI ***shall*** (32) provide messages to the SO and IO that inform them of the system status.

3.1.1.3.2.1 Cold Start-up

The WBI ***shall*** (33) 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 a WBI has been turned off or shutdown, but is still connected to a power source.

3.1.1.3.2.2 Sleep/Standby

The WBI ***shall*** (34) 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 a WBI has been turned on but is not fully functional.

3.1.1.3.2.3 Login Process

The WBI IO station ***shall*** (35) require no more than thirty (30) seconds to complete the login process. The WBI SO station ***shall*** (36) 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 WBI ***shall*** (37) 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 WBI ***shall*** (38) 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 WBI employs a technology that requires recalibration over time, the system ***shall*** (39) employ a calibration process that culminates in a visible notification to clearly indicate to the SO whether the WBI system is correctly calibrated and ready/not ready to scan a passenger. The calibration process ***shall*** (40) take place as necessary in order to keep the system accurate to its qualified detection tier. The WBI ***shall*** (41) provide a message indicating to the operator that re-calibration is necessary and ***shall*** (42) not allow passengers to be scanned by the system during the calibration process.

3.1.1.3.4 Emergency Stop

The WBI ***shall*** (43) include a physical emergency stop (E-Stop) button with protective guards to prevent accidental initiation of an emergency stop. An E-Stop button ***shall*** (44) be located at the SOCP. When an E-Stop button is enabled anywhere on the system, the E-Stop location ***shall*** (45) be identified on the SO and IO stations. Activation of the E-Stop button ***shall*** (46) render the WBI incapable of scanning passengers.

3.1.1.3.5 Lock Down

The WBI system ***shall*** (47) have a lock-down mode so that when activated by the SO:

(a) No portion of the system ***shall*** (48) move under power.

(b) System ***shall*** (49) not allow any passengers to be screened.

(c) System ***shall*** (50) not emit scanning source radiation

(d) System ***shall*** (51) not disable the display monitor or any means of two-way communication.

3.1.1.3.6 Network Interface

The WBI system:

(a) ***Shall*** (52) possess an Ethernet network interface equipped with an RJ-45 connector.

(b) ***Shall*** (53) support full/half duplex data rates of 10/100 mega-bits per second to support future requirements.

(c) ***Shall*** (54) support Transmission Control Protocol / Internet Protocol (TCP/IP).

3.1.1.3.7 External Interface

3.1.1.3.7.1 STIP Interface

The WBI ***shall*** (55) meet the requirements specified in the Security Technology Integrated Program (STIP) Transportation Security Equipment (TSE), Interface Requirements Document (IRD), Version 3.11, 14 April 2008 and STIP Business Rules Document (BRD), 13 August 2007.

The WBI ***shall*** (56) comply with the levels of access control as defined in the User Access Levels and Capabilities appendix.

3.1.1.4 Operator Stations

3.1.1.4.1 Screening Operator Station (SO Station)

The SO station:

(a) ***shall*** (57) 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*** (58) have an activation button to initiate a scan. The activation button, if tethered to the device, ***shall*** (59) provide a minimum of 3 meters of cable length so that the cord does not interfere with the operator's activities.

(c) ***shall*** (60) provide a hard-wired, secure means of communication between IO and SO. An audible means ***shall*** (61) be provided to communicate anomaly presence and location. A visual indicator ***shall*** (62) provide the SO with notification regarding passenger status. A green status indicator ***shall*** (63) be used to denote when passenger is cleared. A red status indicator ***shall*** (64) be used to denote when passenger requires secondary screening. The SO ***shall*** (65) be provided a means to reset the status indicator. This IO/SO communication ***shall*** (66) not be discernible by others.

3.1.1.4.2 Image Operator Station (IO Station)

The WBI IO station ***shall*** (67) include an Image Operator Control Panel (IOCP), which consists of the IO console and any other necessary input devices.

The IO station ***shall*** (68) be operable at a distance up to 100m from the WBI system.

3.1.1.4.2.1 IOCP

The IOCP:

(a) ***shall*** (69) permit only authorized users to log on to the system.

(b) ***shall*** (70) provide a means to indicate clear or suspect status of a passenger.

(c) ***shall*** (71) provide all controls required for the IO to view images.

(d) ***shall*** (72) 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

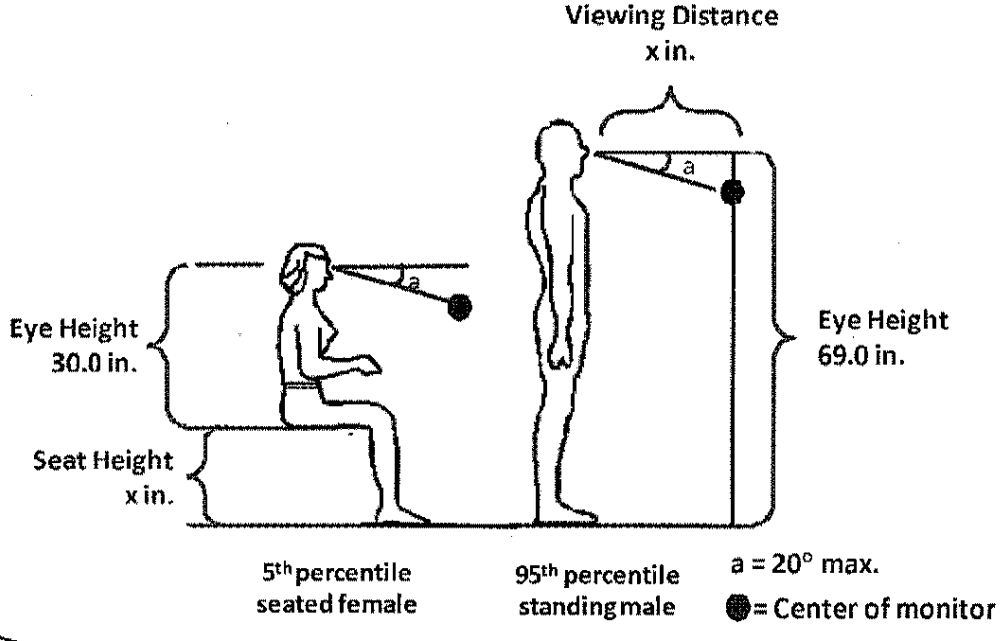
(ii) Zoom from 1X to 4X

3.1.1.4.2.2 IOCP Display Monitor

The IOCP ***shall*** (73) include one or more flat panel color displays each measuring a minimum of 17 inches diagonally.

Mounting for the flat panel displays ***shall*** (74) 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*** (75) be adjustable so that the centers of the monitors range from 110 cm to 160 cm from the surface on which the operator is standing.

These values are based on a seat height of 60 cm and a viewing angle 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*** (76) be easily accessible (visually or physically, as appropriate) from both a standing and seated position within the workstation.

The display monitor mounting method:

(a) ***shall*** (77) allow operators to adjust height, tilt, and viewing angle without requiring the use of tools.

(b) ***shall*** (78) allow for continuous adjustment or in increments of no more than 25 mm

(c) ***shall*** (79) enable adjustments to be accomplished by a single individual

(d) ***shall*** (80) be adjustable to allow a viewing distance from the eye to the display that is not less than 330 mm.

(e) ***shall*** (81) 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*** (82) have the capability to tilt displays up or down between -5° and +20°, in 5° increments or continuously.

(g) ***shall*** (83) 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

(h) ***shall*** (84) allow the monitor(s) to be placed directly in front of the user when the user is in his or her normal working position, whether seated and standing.

(i) ***shall*** (85) 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*** (86) display or indicate, at a minimum, the following:

(a) Current operational state of the WBI system.

(b) Present operational state of the scanner

(c) Critical system parameters which state the operation of the scanner and the complete WBI.

(d) Identification of the IO.

(e) System error messages and diagnostic results.

(f) WBI images.

3.1.1.4.2.4.1 Image Quality

The images ***shall*** (87) have the resolution necessary for the TSO at the IO station to visually identify any anomalies.

The flat panel display ***shall*** (88) have a manufacturer's luminance rating $\geq$ 150 cd/m2.

3.1.1.4.2.4.2 Jitter and Motion Artifacts

The display monitor ***shall*** (89) exhibit no perceptible jitter or motion artifacts.

3.1.1.5 Field Data Reporting System

The WBI:

(a) ***shall*** (90) 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*** (91) collect FDRS data related to system events specifically defined for WBI in the Security Technology Integrated Program (STIP) Transportation Security Equipment (TSE) Interface Requirements Document, Version 3.11, 14 April 2008, Section 2.4.1.

(c) ***shall*** (92) collect FDRS data as identified in Appendix B.

(d) ***shall*** (93) display FDRS reports identified in Appendix E on the IO monitor.

(e) ***shall*** (94) provide User Access data according to the access levels defined in the User Access Levels and Capabilities appendix.

(f) ***shall*** (95) make FDRS raw data available for downloading.

(g) ***shall*** (96) make FDRS data reports available for downloading.

(h) ***shall*** (97) 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 WBI system ***shall*** (98) provide capabilities for data transfers via USB devices. These devices ***shall*** (99) 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*** (100) be installed to permit data uploads and downloads. All necessary software drivers and operating system services to support the data collection devices ***shall*** (101) be preinstalled and preconfigured.

3.1.1.6 Operational Test Kit (OTK)

The vendor ***shall*** (102) provide an OTK that will validate the WBI is operating as required.

3.1.2 Electrical

The WBI:

(a) ***shall*** (103) be capable of operating on commercially available 110 VAC, 220 VAC, or 480 VAC power at 60 Hz with a +/- 15% voltage tolerance and up to a +/- 10% variance in frequency, at no more than 20 amp service for 110 VAC, 10 amp for 220 VAC, or 5 amp for 480 VAC.

(b) ***shall*** (104) route the power and data cables (if applicable) to floor level.

(c) ***shall*** (105) meet the input power requirements defined in Appendix D, TSA Operational Power Requirements.

3.1.2.1 Uninterruptible Power Supply

The WBI system ***shall*** (106) include an Uninterruptible Power Supply (UPS) to ensure automatic, orderly, and safe shut-down of WBI system equipment and to preserve data in the event of loss of

electrical power. The UPS ***shall*** (107) provide an indicator to the operator when running on UPS power and ***shall*** (108) 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 WBI system ***shall*** (109) not exceed 416.04 kg/m2 (85 lbs/ft^2) based on the actual foot print dimensions. The point load (concentrated load) ***shall*** (110) not exceed 453.59 kg over a 193.55 cm square (1,000 lbs over a 30 in square) floor area. The vendor ***shall*** (111) 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 WBI system footprint ***shall*** (112) be less than 4 square meters.

3.1.3.2.2 Orientation

The WBI system ***shall*** (113) be configurable so that passengers may face left or right in relation to the entrance during scanning.

3.1.3.2.3 Height

The WBI system height ***shall*** (114) be less than 3 m.

3.1.3.2.4 Width

The WBI system width ***shall*** (115) be no greater than 2.25 m.

3.1.4 Identification Markings

3.1.4.1 Identification Information

The WBI system ***shall*** (116) identify the following information (which ***shall*** (117) 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*** (118) be as permanent as the life expectancy of the item and ***shall*** (119) be capable of withstanding the environmental tests and cleaning procedures specified for the item to which it is affixed. Legibility ***shall*** (120) be understood to mean that which allows ready human or machine readability, as applicable. Information contained on identification plates ***shall*** (121) be displayed in a color that contrasts to the color of the surface of the plate. Identification tag marking, when used, ***shall*** (122) be permanent to the extent required for use of the item. The minimum text character height ***shall*** (123) be 2.54 mm (0.1 inch).

3.1.5 Environmental

3.1.5.1 Operational Environment

The WBI ***shall*** (124) 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 WBI system ***shall*** (125) 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 WBI ***shall*** (126) be capable of storage under these conditions for not less than 12 months, without resulting in any temporary or permanent degradation of WBI 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*** (127) 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 WBI system:

(a) ***shall*** (128) 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.

(iii) Assuming 8 to 10 equipment discharge test points plus coupling planes, positive and negative discharge waveform polarities.

(b) ***shall*** (129) 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*** (130) 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*** (131) 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*** (132) 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*** (133) 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*** (134) 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

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 WBI system vendor ***shall*** (135) provide a report indicating that the WBI 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 WBI components with a user interface:

(a) ***shall*** (136) 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*** (137) use a graphical user interface (GUI) that is viewable on the WBI display monitor and controlled through the IOCP.

(c) During utilization of the WBI:

(i) The system ***shall*** (138) 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*** (139) be used consistently across displays.

(iii) Key strokes ***shall*** (140) not be buffered.

(iv) The system ***shall*** (141) 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*** (142) appear in the same location across screens.

(vi) The system ***shall*** (143) 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*** (144) 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*** (145) 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.

3.1.7.1 Noise

Audible noise levels produced by the WBI ***shall*** (146) not exceed a time-weighted average of 70 dBA within 1 m from the WBI system over a 5 minute period.

3.1.8 Regulatory

3.1.8.1 Electromagnetic Emission Safety

The WBI system ***shall*** (147) 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 WBI System radio frequency emissions ***shall*** (148) comply with 47 CFR 15, Radio Frequency Devices.

3.1.9 Reliability, Maintainability, and Availability

3.1.9.1 Reliability

The WBI system ***shall*** (149) 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 WBI system ***shall*** (150) be designed to have a Mean Time To Repair (MTTR) of not more than 4 hours. MTTR is defined as follows:

MTTR = Total Active Corrective Maintenance Time / Number of Maintenance Actions

3.1.9.2.1 Maintenance Access

The WBI system ***shall*** (151) 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*** (152) be either removable or sliding with a key lock and handles.

3.1.9.2.2 Scheduled (Preventive) Maintenance

The WBI system ***shall*** (153) have a Mean Time Between Maintenance Action (MTBMA) for scheduled (preventive) maintenance of not less than seven (7) days. The maintenance manual ***shall*** (154) specify all scheduled maintenance activities and the intervals of performance.

The WBI system ***shall*** (155) not require any custom tools for the performance of scheduled maintenance.

3.1.9.2.3 Unscheduled (Corrective) Maintenance

The WBI system:

Shall (156) be modular in design to allow easy removal and replacement of failed Line Replaceable Units (LRUs).

(a) Must provide Built In Testing (BIT) diagnostic capabilities that:

(i) ***shall*** (157) initiate on power-up.

(ii) ***shall*** (158) monitor system health in a non-interference (background) mode during normal operations.

(iii) ***shall*** (159) capture and report error and failure codes to the FDRS.

(b) Must provide Fault Isolation Test (FIT) diagnostic capabilities that:

(i) ***shall*** (160) be manually initiated by the TSO as a result of BIT or other system-generated error.

(ii) ***shall*** (161) identify the failed LRU with at least 90% accuracy.

(iii) ***shall*** (162) be at least 98% accurate when isolating the failed component to one of three LRUs.

(iv) ***shall*** (163) 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 WBI system ***shall*** (164) demonstrate an inherent availability (A_i) threshold of at least 99%. Availability ***shall*** (165) 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 / Failure rate

Failure Rate = Number of failures / Total Operating Hours

3.1.10 Safety

3.1.10.1 General

The WBI ***shall*** (166) not expose operators, passengers, or maintenance personnel to hot surfaces over 43.9 degrees Celsius (111 degrees Fahrenheit).

3.1.10.2 Radiation

The WBI ***shall*** (167) comply with ANSI/HPS N43.17-2002 American National Standard – "Radiation Safety for Personnel Security Screening Systems Using X-ray."

The WBI ***shall*** (168) comply with OSHA Standard, 29 CFR 1910.1096, Ionizing Radiation, 1 January 2007.

The WBI ***shall*** (169) 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 WBI ***shall*** (170) 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 1988.

3.1.10.3 Electrical Safety

The WBI:

(a) ***shall*** (171) 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*** (172) comply with UL 61010A-1, *Electrical Equipment for Laboratory Use,* Part 1: General Requirements, 30 January 2002.

(c) ***shall*** (173) 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 WBI:

(a) ***shall*** (174) possess no sharp corners or edges that can puncture, cut, or tear the skin or clothing, or otherwise cause bodily injury.

(b) ***shall*** (175) 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*** (176) possess no loose covers and cowlings.

3.1.10.5 Hazardous Materials

If hazardous materials are used in the WBI, they ***shall*** (177) be identified, including their location and amount by weight or volume. A complete Material Safety Data Sheet (MSDS) ***shall*** (178) be developed and provided to meet the requirements of 29 CFR 1910.1200, OSHA Hazard Communication. The

hazardous materials ***shall*** (179) 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 WBI system:

(a) ***shall*** (180) provide the means to physically protect its sensitive components and controls.

(b) ***shall*** (181) possess highly visible tamper-evident seals or alarms on assemblies that contain sensitive components/data.

3.1.11.2 Software Access

The WBI:

(a) ***shall*** (182) allow user access, password protection, and capabilities per the User Access Levels and Capabilities appendix.

(b) ***shall*** (183) 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*** (184) through the use of a graphical user interface (GUI) or menu, allow the user to encrypt and export a user database.

(d) ***shall*** (185) 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 WBI system ***shall*** (186) 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

b2 b3

3.2.1.1.1 System Detection

Detection performance requirements are as follows:

3.2.1.1.1.1 Explosives

4(i)

The WBI System ***shall*** (187) produce images to enable an operator to determine the presence and location of explosives [redacted]

3.2.1.1.1.2 Weapons

The WBI System ***shall*** (188) produce images to enable an operator to determine the presence and location of weapons [redacted]

3.2.1.1.1.3 Liquids

(4)(i)

The WBI System ***shall*** (189) produce images to enable an operator to determine the presence and location of liquids, [redacted]

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 WBI System ***shall*** (190) produce images to enable an operator to determine the presence and location of explosives, [redacted]

3.3.1.1.1.2 Weapons

The WBI System ***shall*** (191) produce images to enable an operator to determine the presence and location of weapons [redacted]

3.3.1.1.1.3 Liquids

The WBI System ***shall*** (192) produce images to enable an operator to determine the presence and location of liquids [redacted]

3.4 OPTIONAL CAPABILITIES

3.4.1 Automated Threat Detection Marking

The WBI system ***shall*** (193) provide an automated detection highlighting function in meeting the tiered detection requirements.

Automated detection highlighting of anomalies ***shall*** (194) be coded red.

Automated detection highlighting ***shall*** (195) be bounded by a box indicating the location of the anomaly.

The WBI ***shall*** (196) provide a means for the IO to toggle automated detection highlighting on and off.

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 a WBI 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 a WBI has met the requirements of the WBI 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 WBI systems to verify operational effectiveness, suitability, reliability, and availability of the equipment. Continuous assessment will include collection of data from fielded WBI for the purpose of assessing field performance over time.

4.2 VERIFICATION METHODS

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

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 WBI 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.

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	3.1.1.3.1.1.1	Multiplexing	D	X	D	
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	

26	3.1.1.3.1.2	Test Mode	D	D	X	
27	3.1.1.3.1.2	Test Mode	D	X	X	
28	3.1.1.3.1.2	Test Mode	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	Start-up and Power-Down	D	D	X	
33	3.1.1.3.2.1	Cold Start-up	D	D	X	
34	3.1.1.3.2.2	Sleep / Standby	D	D	X	
35	3.1.1.3.2.3	Login Process	D	D	X	
36	3.1.1.3.2.3	Login Process	D	D	X	
37	3.1.1.3.2.4	Fault Reset	D	D	X	
38	3.1.1.3.2.5	Power-Down	D	D	X	
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	3.1.1.3.3	Calibration	D	D	D	
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	I	I	X	
46	3.1.1.3.4	E-Stop	D	D	D	
47	3.1.1.3.5	Lock Down	D	X	X	
48	3.1.1.3.5	Lock Down	T	T	X	
49	3.1.1.3.5	Lock Down	T	X	X	
50	3.1.1.3.5	Lock Down	T	X	X	
51	3.1.1.3.5	Lock Down	T	T	X	
52	3.1.1.3.6	Network Interface	I	I	X	
53	3.1.1.3.6	Network Interface	A	X	X	
54	3.1.1.3.6	Network Interface	A	X	X	
55	3.1.1.3.7.1	STIP Interface	A	X	X	

56	3.1.1.3.7.1	STIP Interface	A	X	X	
57	3.1.1.4.1	SO Station	I	I	I	
58	3.1.1.4.1	SO Station	I	I	X	
59	3.1.1.4.1	SO Station	I	X	X	
60	3.1.1.4.1	SO Station	I	X	X	
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	3.1.1.4.1	SO Station	D	D	D	
65	3.1.1.4.1	SO Station	D	D	D	
66	3.1.1.4.1	SO Station	D	D	D	
67	3.1.1.4.2	IO Station	I	X	X	
68	3.1.1.4.2	IO Station	D	X	X	
69	3.1.1.4.2.1	IOCP	T	X	X	C-C
70	3.1.1.4.2.1	IOCP	D	X	X	
71	3.1.1.4.2.1	IOCP	D	X	X	
72	3.1.1.4.2.1	IOCP	D	X	X	
73	3.1.1.4.2.2	IOCP Display Monitor	I	X	X	
74	3.1.1.4.2.2	IOCP Display Monitor	I	I	I	
75	3.1.1.4.2.2	IOCP Display Monitor	I	I	I	
76	3.1.1.4.2.3	Display Monitor Mounting	D	D	D	
77	3.1.1.4.2.3	Display Monitor Mounting	D	D	D	
78	3.1.1.4.2.3	Display Monitor Mounting	T	X	X	
79	3.1.1.4.2.3	Display Monitor Mounting	D	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	T	X	X	
82	3.1.1.4.2.3	Display Monitor Mounting	T	X	X	
83	3.1.1.4.2.3	Display Monitor Mounting	T	X	X	
84	3.1.1.4.2.3	Display Monitor Mounting	D	D	D	
85	3.1.1.4.2.3	Display Monitor Mounting	I	I	I	
86	3.1.1.4.2.4	Operator Display	I	I	I	
87	3.1.1.4.2.4.1	Image Quality	I	I	X	
88	3.1.1.4.2.4.1	Image Quality	I	X	X	
89	3.1.1.4.2.4.2	Jitter and Motion Artifacts	I	X	X	
90	3.1.1.5	Field Data Reporting System	D	X	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	D	X	X	
94	3.1.1.5	Field Data Reporting System	D	D	X	
95	3.1.1.5	Field Data Reporting System	D	X	X	

96	3.1.1.5	Field Data Reporting System	D	X	X	
97	3.1.1.5	Field Data Reporting System	A	X	X	
98	3.1.1.5.1	Data Storage / Transfer	D	D	D	
99	3.1.1.5.1	Data Storage / Transfer	D	D	D	
100	3.1.1.5.1	Data Storage / Transfer	I	I	X	
101	3.1.1.5.1	Data Storage / Transfer	I	X	X	
102	3.1.1.6	OTK	D	X	X	
103	3.1.2	Electrical	T	X	X	
104	3.1.2	Electrical	D	D	D	
105	3.1.2	Electrical	T	X	X	
106	3.1.2.1	Uninterruptible Power Supply	D	I	I	
107	3.1.2.1	Uninterruptible Power Supply	D	D	X	
108	3.1.2.1	Uninterruptible Power Supply	D	X	X	
109	3.1.3.1	Floor Loading	A	X	X	
110	3.1.3.1	Floor Loading	A	X	X	
111	3.1.3.1	Floor Loading	A	X	X	
112	3.1.3.2.1	Footprint	I	X	X	
113	3.1.3.2.2	Orientation	D	X	X	
114	3.1.3.2.3	Height	I	X	X	
115	3.1.3.2.4	Width	I	X	X	
116	3.1.4.1	ID Info.	I	X	X	
117	3.1.4.1	ID Info.	I	X	X	
118	3.1.4.2	Permanency and Legibility	A	X	X	
119	3.1.4.2	Permanency and Legibility	T	X	X	

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

142	3.1.7	Human Factors	I	X	X	
143	3.1.7	Human Factors	I	X	X	
144	3.1.7	Human Factors	I	X	X	
145	3.1.7	Human Factors	D	X	X	
146	3.1.7.1	Noise	T	X	X	
147	3.1.8.1	Electromagnetic Emission Safety	A	X	X	C-I
148	3.1.8.2	Emission Control	A	X	X	C-I
149	3.1.9.1	Reliability	A	X	X	C-C
150	3.1.9.2	Maintainability	A	X	X	C-C
151	3.1.9.2.1	Maintenance Access	I	I	X	
152	3.1.9.2.1	Maintenance Access	I	X	X	
153	3.1.9.2.2	Scheduled Maintenance	A	X	X	
154	3.1.9.2.2	Scheduled Maintenance	A	X	X	
155	3.1.9.2.3	Scheduled Maintenance	A	X	X	
156	3.1.9.2.3	Unscheduled Maintenance	I	X	X	
157	3.1.9.2.3	Unscheduled Maintenance	D	X	X	
158	3.1.9.2.3	Unscheduled Maintenance	D	X	X	
159	3.1.9.2.3	Unscheduled Maintenance	D	X	X	
160	3.1.9.2.3	Unscheduled Maintenance	D	X	X	
161	3.1.9.2.3	Unscheduled Maintenance	T	X	X	
162	3.1.9.2.3	Unscheduled Maintenance	T	X	X	
163	3.1.9.2.3	Unscheduled Maintenance	D	X	X	
164	3.1.9.3	Availability	A	X	X	C-C

165	3.1.9.3	Availability	A	X	X	C-C
166	3.1.10.1	General	T	T	X	
167	3.1.10.2	Radiation	A	X	X	C-I
168	3.1.10.2	Radiation	A	X	X	C-I
169	3.1.10.2	Radiation	A	X	X	C-I
170	3.1.10.2	Radiation	A	X	X	C-I
171	3.10.1.3	Electrical Safety	A	X	X	C-I
172	3.10.1.3	Electrical Safety	A	X	X	C-I
173	3.10.1.3	Electrical Safety	A	X	X	C-I
174	3.1.10.4	Ergonomic Safety	I	I	X	
175	3.1.10.4	Ergonomic Safety	I	I	X	
176	3.1.10.4	Ergonomic Safety	I	X	X	
177	3.1.10.5	Hazardous Materials	I	X	X	
178	3.1.10.5	Hazardous Materials	A	X	X	
179	3.1.10.5	Hazardous Materials	I	X	X	
180	3.1.11.1	Physical Security	I	I	X	
181	3.1.11.1	Physical Security	I	I	X	
182	3.1.11.2	Software Access	D	X	X	
183	3.1.11.2	Software Access	A	X	X	
184	3.1.11.2	Software Access	D	D	X	
185	3.1.11.2	Software Access	D	D	X	
186	3.1.11.3	Info. Tech. Security	A	X	X	
187	3.2.1.1.1.1	Explosives	A	X	X	Q-T

188	3.2.1.1.1.2	Weapons	A	X	X	Q-T
189	3.2.1.1.1.3	Liquids	A	X	X	Q-T
190	3.3.1.1.1.1	Explosives	A	X	X	Q-T
191	3.3.1.1.1.2	Weapons	A	X	X	Q-T
192	3.3.1.1.1.3	Liquids	A	X	X	Q-T
193	3.4.1	Automated Threat Detection Marking	D	X	X	
194	3.4.1	Automated Threat Detection Marking	D	X	X	
195	3.4.1	Automated Threat Detection Marking	D	X	X	
196	3.4.1	Automated Threat Detection Marking	D	X	X	
Appendix C						
197	n/a	User Access Levels and Capabilities	A	X	X	
Appendix D						
198	5.1	Baseline Voltage and Current Distortion	A	X	X	C-I
199	5.1	Baseline Voltage and Current Distortion	A	X	X	C-I
200	5.2	Power Usage Profile and Power Factor	A	X	X	C-I
201	5.3	Maximum Inrush Current Ration	A	X	X	C-I
202	5.4	Steady State Current Unbalance	A	X	X	C-I

203	5.4	Steady State Current Unbalance	A	X	X	C-I
204	5.4	Steady State Current Unbalance	A	X	X	C-I
205	5.4	Steady State Current Unbalance	A	X	X	C-I
206	5.5	Maximum Leakage Current	A	X	X	C-I
207	5.6	Voltage Sag and Interruption Withstand Performance	A	X	X	C-I
208	5.7	Uninterruptible Power Supply	A	X	X	C-I
Appendix E						
209	1.0	FDRS Report Display	D	X	X	
210	1.0	FDRS Report Display	D	X	X	
211	1.1	IO Log Report	D	X	X	
212	1.1	IO Log Report	D	X	X	
213	1.1	IO Log Report	D	X	X	
214	1.2	Event Report	D	X	X	
215	1.2	Event Report	D	X	X	
216	1.2	Event Report	D	X	X	
217	1.2	Event Report	D	X	X	
218	1.3	Access History	D	X	X	
219	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	

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)

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

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
WBI	Whole Body Imager

APPENDIX A TECHNOLOGY SECURITY REQUIREMENTS

Prepared for:

Transportation Security Administration
Security Transportation Deployment Office

January 2008

A.1 INTRODUCTION

Due to the TSA's plan for a secure network which will connect the vast information systems of our nation's airports, it is necessary to outline information security control requirements to ensure the network is both secure and effective. In support of the Security Technology Integration Program (STIP) team's work to achieve this goal through the High Speed Operational Connectivity (Hi-SOC) roll-out, the Certification and Accreditation (C&A) Assessment team compiled these requirements in the form of an IT Security (ITSEC) Requirements matrix which applies to all Transportation Security Equipment (TSE).

The points of contact for this effort are as follows:

[redacted]nformation System Security Officer (ISSO) b6 [redacted]
U.S. Transportation Security Administration
701 South 12th Street
Arlington, VA 22202
Phone: (202) 28[redacted] b2
Email: [redacted]ihs.gov

A.2 SCOPE

This document covers a subset of the security requirements mandated by DHS and TSA. The complete set of IT Security requirements can be found in the TSA Management Directive 1400.3 and the DHS National Security Systems Handbook 4300.A. This document was created to identify specific requirements from the full set of security requirements that are directly applicable to the hardware and software utilized for the TSE being designed and built.

A.3 VENDOR REQUIREMENTS

Vendors **shall** configure their Operating System (OS) and application software by strictly following the OS Secure Baseline Configuration Guides. All hardware and software systems **shall** be secured based on the TSA IT Security requirements which can be found in the TSA Management Directive 1400.3 and the DHS National Security Systems Handbook 4300.A.

Technology Security Requirements are also included in section 6, which provides a guideline to assisting an implementing the major security requirements. This document provides a reference of many of the findings that have been identified in past security scans. These requirements are included as guideline which TSE is required to meet all of the security requirements identified in 1400.3 and the 4300.A TSA and DHS IT Security Requirements documents. Additionally, TSA will conduct preliminary security scans (as needed and as requested) and quarterly security scans on the equipment that provides security reports. This will help the vendor in meeting the security requirements.

A.4 REFERENCES

The following documents were utilized in the development of this set of Systems ITSEC Requirements for Systems Developers & Administrators:

TSA MD 1400.3	Transportation Security Administration (TSA) Management Directive No. 1400.3 - TSA Information Security Policy
DHS 4300 A	Department of Homeland Security Sensitive Systems Handbook V3.2, October 1, 2005

FIPS 140-2	Security Requirements for Cryptographic Modules – December 3, 2002 (Change Notice 2)
Public Law 107-296	Homeland Security Act of 2002 - November 25, 2002
FISMA 2002	Federal Information Security Management Act (FISMA) of 2002 - November 25, 2002
Public Law 104-106	Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)] – February 10, 1996
HSAR	Homeland Security Acquisition Regulation – December 2003

A.5 OS HARDENING/SECURITY REQUIREMENTS

Original Equipment Manufacturer (OEM) vendors should follow the OS Secure Baseline Configuration Guides from the following sources and in the following order (i.e., if an OS guide is not available under source i. then go to source ii.):

i. TSA
   OS Secure Baseline Configuration Guides available from TSA upon request are:
   1. HP-UX Server Secure Baseline
   2. Linux Server Secure Baseline
   3. Solaris Server Secure Baseline
   4. Windows 2000 Server Secure Baseline
   5. Windows 2003-XP Secure Baseline

ii. Department of Homeland Security (DHS)

iii. National Security Agency (NSA)
   http://www.nsa.gov/snac/index.cfm?MenuID=scg10.3.1

iv. Defense Information Security Agency (DISA)
   http://iase.disa.mil/stigs/checklist/index.html

v. National Institute of Standards and Technology (NIST)
   http://csrc.nist.gov/pcig/cig.html

A.6 SYSTEMS IT SECURITY REQUIREMENTS

*Reference numbers apply to this document only.

**A waiver is requested when a requirement cannot be met within a reasonable timeframe, but can be fixed within a near-future timeframe (for example, 6 months to a year).

***An exemption is requested for a requirement that cannot reasonably be fixed ever. This is something that will either be an unreasonable cost to fix or fixing the issue would result in the equipment not working and there is no work-around for the fix.

Please fill in the matrix below for the following requirements. If a requirement has been met, please indicate Yes. If the requirement has not been met, please indicate No and under the Notes section please fill out the reason why. If a requirement is Not Applicable, please indicate this with N/A and under the Notes section please fill out the reason why. If requirements cannot be met, please provide a detailed explanation in either the waiver or the exemption sections of the matrix.

*Reference Number	Control Category	DHS or TSA Reference	Systems IT Security Requirement	Met Requirement Yes/No or N/A	Notes No or N/A, Other	**Waiver Explanation	***Exemption Explanation
AC-1	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 7 "Passwords" Section 3.2.1, Parts A and L	Password length shall be a minimum of eight (8) characters and a maximum of 15 characters.				
AC-2	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 7 "Passwords" Section 3.2.1, Part B	Passwords shall contain at least one of each of the following: one alphabetic uppercase, one alphabetic lowercase, one numeric, and one special character.				
AC-3	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 7 "Passwords"	Passwords shall not contain any two identical consecutive characters.				

*Reference Number	Control Category	DHS or TSA Reference	Systems IT Security Requirement	Met Requirement Yes/No or N/A	Notes No or N/A, Other	**Waiver Explanation	***Exemption Explanation
		Section 3.2.1, Part C					
AC-4	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 7 "Passwords" Section 3.2.1, Part K	Passwords shall not be the same as the User ID.				
AC-5	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 7 "Passwords" Section 3.2.2, Part A	Passwords shall have a maximum lifetime of 90 days.				
AC-6	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 7 "Passwords" Section 3.2.2, Part B	Passwords shall not be reused for a minimum of 6 password change cycles.				
AC-7	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 7 "Passwords" Section 3.6, Part A	Systems, applications and network components sometimes come with default system accounts and passwords (or no password). The TSA requires that:				
AC-8	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 7 "Passwords" Section 3.6, Part A	All default accounts shall be removed from the system and the default password must be changed prior to placing the system or device into service.				

*Reference Number	Control Category	DHS or TSA Reference	Systems IT Security Requirement	Met Requirement Yes/No or N/A	Notes No or N/A, Other	**Waiver Explanation	***Exemption Explanation
AC-9	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 7 "Passwords" Section 3.6, Part A	All system or root level accounts shall have a password assigned prior to placement of the system or device into service.				
AC-10	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 7 "Passwords" Section 3.6, Part A	All "guest" accounts shall be removed from the system.				
AC-11	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 7 "Passwords" Section 3.6, Part A	Operating systems and applications shall be configured to force users to create strong passwords, as defined in this document.				
AC-12	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 7 "Passwords" Section 3.2.7, Part A	Personal passwords shall be authenticated each time a claim of identity is made (e.g., when "logging onto" an interactive system).				
AC-13	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 7 "Passwords" Section 3.2.7,Part B	Access passwords shall be authenticated during the initial request for access to protected data.				

*Reference Number	Control Category	DHS or TSA Reference	Systems IT Security Requirement	Met Requirement Yes/No or N/A	Notes No or N/A, Other	**Waiver Explanation	***Exemption Explanation
AC-14	Access Control	DHS MD 4300, v2.1 Chapter 5, Section 5.6.5, "Internet Security", Part B	Firewalls shall be configured to prohibit any protocol or service that is not explicitly permitted.				
AC-15	Access Control	DHS MD 4300, v2.1, Chapter 5, Section 5.6.5, "Internet Security", Part D	Mobile code (e.g., ActiveX, JavaScript) that has not been reviewed and digitally approved by an appropriate TSA authority shall not be used.				
AC-16	Access Control	DHS MD 4300, v2.1 TSA MD 1400.3, v3.1_r1, Chapter 3, Section 11b, Section 3.3,Part C; and Section 11c , Section 3.4, Part C	Telnet shall not be used to connect to any TSA computer. A connection protocol such as Secure Shell (SSH) that employs secure authentication (two factor, encrypted, key exchange, etc.) and is approved by the Organization Element shall be used instead.				
AC-17	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 2 "Network Logical Access Control" Section 3.2,Part A	Upon successful logon, the user shall be notified of the date and time of the last successful logon using this user identity and the number of unsuccessful logon attempts using this user identity since the last successful logon.				
AC-18	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 2 "Network Logical Access Control" Section 3.2,Part B	Upon successful logon, a standard and approved warning message shall be displayed. Minimum requirements for this message shall be as follows:				

*Reference Number	Control Category	DHS or TSA Reference	Systems IT Security Requirement	Met Requirement Yes/No or N/A	Notes No or N/A, Other	**Waiver Explanation	***Exemption Explanation
			SAMPLE WARNING MESSAGE: "THIS IS AN UNCLASSIFIED SYSTEM. This is a Government information system. This system is for the use of authorized users and unclassified processing only. Individuals using this computer system without authority or in excess of their authority are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity or inappropriate use, such as input of classified information, system personnel may provide the evidence of such monitoring to TSA officials and/or law enforcement officials, depending on the nature of the evidence revealed. Security Violations will be issued to any user processing Classified National Security Information on this system."				
AC-19	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 2 "Network Logical Access Control" Section 3.2,Part B	Warning message shall be displayed until a specific user action is taken.				
AC-20	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 2	Warning message shall include a warning that they have accessed a Government information system.				

*Reference Number	Control Category	DHS or TSA Reference	Systems IT Security Requirement	Met Requirement Yes/No or N/A	Notes No or N/A, Other	**Waiver Explanation	***Exemption Explanation
		"Network Logical Access Control" Section 3.2,Part B					
AC-21	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 2 "Network Logical Access Control" Section 3.2,Part B	Warning message shall include a warning that usage may be monitored, recorded and subject to audit.				
AC-22	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 2 "Network Logical Access Control" Section 3.2,Part B	Warning message shall include a warning that notifies users that use indicates consent to monitoring and recording.				
AC-23	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 2 "Network Logical Access Control" Section 3.2,Part B	Warning message shall include a warning that notifies users that unauthorized use is prohibited and subject to criminal and civil penalties.				
AC-24	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 2 "Network Logical Access Control" Section 3.3,Part A	All end user assets shall have and employ session lock capabilities in accordance with TSA MD 1400.3, End User Assets Policy.				

*Reference Number	Control Category	DHS or TSA Reference	Systems IT Security Requirement	Met Requirement Yes/No or N/A	Notes No or N/A, Other	**Waiver Explanation	***Exemption Explanation
AC-25	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 2 "Network Logical Access Control" Section 3.4,Part A	All end user assets shall have and employ session inactivity lockout capabilities in accordance with TSA MD 1400.3, End User Assets Policy.				
AC-26	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 3 "Remote Access" Section 3, Parts D and J	Remote access shall require identification and authentication consisting of a user identity and password and shall not be connected to any other network aside from the TSA network.				
AC-27	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 3 "Remote Access" Section 3, Part M	Split-tunneling or dual homing shall not be permitted at any time; only one connection is allowed.				
AC-28	Access Control	DHS MD 4300, v2.1, Chapter 4, Section 4.6.2, "Wireless LANs", Part A; TSA MD 1400.3, v3.1_r1, Chapter 4, Section 4 "Wireless Access" Section 3, Part A	Wireless communications technologies are prohibited from use within DHS unless the DHS CISO specifically approves the technology and application. [If the device is equipped with wireless technology, this requirement must be met and this technology MUST be disabled on the device]				

*Reference Number	Control Category	DHS or TSA Reference	Systems IT Security Requirement	Met Requirement Yes/No or N/A	Notes No or N/A, Other	**Waiver Explanation	***Exemption Explanation
AC-29	Access Control	DHS MD 4300, v2.1, Chapter 5, Section 5.3, "Identification and Authentication", Part B	For IT systems requiring authentication controls, the IT system shall ensure that each user is authenticated before IT system access occurs.				
AC-30	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 2 "Network Logical Access Control" Section 3.7, Part A	Each system will be configured to restrict a user or process to the least privileges or access required to perform authorized tasks.				
AC-31	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 7 "Passwords" Section 3.2.6, Part C	Unencrypted passwords shall be transmitted as ASCII characters if interchanged between TSA IT systems within the TSA Wide Area Network and shall be transmitted separate from any identification of intended use. Encrypted passwords and virtual passwords shall be transmitted either as a 64-bit binary field in bit-oriented communications, or as ASCII representations of the hexadecimal character set (i.e., the 16 characters in the set [0-9, AF] in character-oriented communications).				
AC-32	Access Control	TSA MD 1400.3, v3.1_r1, Chapter 3,	VPN assets shall be automatically disconnected from the TSA network after				

*Reference Number	Control Category	DHS or TSA Reference	Systems IT Security Requirement	Met Requirement Yes/No or N/A	Notes No or N/A, Other	**Waiver Explanation	***Exemption Explanation
		Section 11d "VPN Security" Section 3.2, Part F	thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes used to keep the connection open are prohibited.				
AC-32	Access Control	DHS 4300A, v3.2, Chapter 5.0, Section 5.4.5, "Network Security", Part F	File Transfer Protocol (FTP) shall not be used to connect to or from any DHS computer. FTP shall be disabled on the device.				
AU-1	Audit and Accountability	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 10 "Security Audit Trails" Section 3, Part A	All devices capable of logging shall have logging enabled at all times.				
AU-2	Audit and Accountability	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 10 "Security Audit Trails" Section 3, Part C	All successful and unsuccessful attempts to access TSA networks, network devices, software applications, and systems shall be logged automatically to an appropriate log file by the component's logon process.				
AU-3	Audit and Accountability	TSA MD 1400.3, v3.1_r1, , Chapter 4, Section 10 "Security Audit Trails" Section 3, Part D	Audit trails shall contain at a minimum, the identity of each user and device accessing or attempting to access an information technology (IT) system or network component; the time and date of the access and the logoff; activities that				

*Reference Number	Control Category	DHS or TSA Reference	Systems IT Security Requirement	Met Requirement Yes/No or N/A	Notes No or N/A, Other	**Waiver Explanation	***Exemption Explanation
			might modify, bypass, or negate IT security safeguards; and security-relevant actions associated with processing.				
AU-4	Audit and Accountability	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 10 "Security Audit Trails" Section 3, Part J	Individual audit trail records shall specify the authenticated identity of the individual or process generating the record.				
AU-5	Audit and Accountability	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 10 "Security Audit Trails" Section 3, Part J	Individual audit trail records shall specify the software or system command used to initiate the event.				
AU-6	Audit and Accountability	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 10 "Security Audit Trails" Section 3, Part J	Individual audit trail records shall be time stamped, accurate to within a second or less of the TSA network time reference, and include local time zone information.				
AU-7	Audit and Accountability	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 10 "Security Audit Trails" Section 3, Part K	Password files shall be encrypted or hashed when stored in logs.				
AU-8	Audit and Accountability	TSA MD 1400.3, v3.1_r1, Chapter 4, Section 10	The information system shall provide the capability to ensure that audit trails and audit logs are protected against				

*Reference Number	Control Category	DHS or TSA Reference	Systems IT Security Requirement	Met Requirement Yes/No or N/A	Notes No or N/A, Other	**Waiver Explanation	***Exemption Explanation
		"Security Audit Trails" Section 3 Part H	unauthorized alteration, loss, unavailability, disclosure, or destruction.				
AU-9	Audit and Accountability	DHS Windows Server 2003/Windows XP Secure Baseline Configuration Guide, Section 2 "Audit Trail Controls"	Auditing shall be implemented in accordance with DHS Secure Configuration Baseline Guide for the information system Operating System.				
IA-1	Identification and Authentication	TSA MD 1400.3, v3.1_r1, Chapter 1, "General Information Security Policy", Section 5.1.3.9	The information system shall provide the capability to uniquely identify and authenticate users prior to each network session. This includes access to individual, group, and functional or service accounts. The positive identification must be verified through strong authentication methods (e.g., password, biometric, token, certificate, etc.).				
SI-1	System and Information Integrity	DHS MD 4300, v2.1, Chapter 5, Section 5.8, "Virus Protection", Part A	The information system shall implement antivirus software at the desktop that is properly configured to check all files.				
SI-2	System and Information Integrity	DHS MD 4300, v2.1, Chapter 5, Section 5.8, "Virus Protection", Part A	The information system shall install updates to antivirus software and signature files in a timely and expeditious manner without requiring the end user to specifically request the update.				

*Reference Number	Control Category	DHS or TSA Reference	Systems IT Security Requirement	Met Requirement Yes/No or N/A	Notes No or N/A, Other	**Waiver Explanation	***Exemption Explanation
SI-3	System and Information Integrity	TSA MD 1400.3, v3.1_r1, Chapter 3, Section 11 "Infrastructure Asset Security" Section 3, Part H	All initialization, shutdown, and abort sequences and scripts shall be configured to ensure the network remains in a secure state.				

APPENDIX B FIELD DATA REPORTING SYSTEM REQUIREMENTS

DATA ELEMENTS

The data elements to be collected by the WBI 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 WBI 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 WBI	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 WBI System serial number).
User_ID	Identification login of the IO	String (length = 15)	
FirstName	IO First Name	String (length = 15)	
LastName	IO Last Name	String (length = 15)	
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 during session	Integer	

Field Name	Field Description	Field Format	Field Values/Comments
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"
WBIModelNo	Model Number of the WBI System	String (length = 8)	

TABLE II. System Event Information.

Field Name	Field Description	Field Format	Field Values/Comments
MACHINE_ID	Identification number of the WBI 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).
WBIModelNo	Model Number of the WBI 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	WBI software version identification	String (length = 10)	Contractor assigned software version identification for the software running on the WBI System
User_ID	Identification login of the IO	String (length = 15)	
FirstName	IO Name	String (length = 15)	
LastName	IO Name	String (length = 15)	
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, system shutdown.

TABLE III. Access History Information.

Field Name	Field Description	Field Format	Field Values/Comments
MACHINE_ID	Identification number of the WBI 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

TABLE IV. Scan Information.

Field Name	Field Description	Field Format	Field Values/Comments
MACHINE_ID	Identification number of the WBI	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 WBI System serial number).
SoftVers	WBI software version identification	String (length = 10)	Contractor assigned software version identification for the software running on the WBI 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)	

TABLE V. User Data File.

Field Name	Field Description	Field Format	Field Values/Comments
FirstName	TSO Name	String (length = 15)	
LastName	TSO Name	String (length = 15)	
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

APPENDIX C USER ACCESS LEVELS AND CAPABILITIES

User access and associated capabilities, based on username, password, and user access level, ***shall*** (197) 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 Modify Access Level Capabilities 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 Note 1: 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 WBI FDRS Database and Reports Access and view WBI User Database Download WBI FDRS Data Calibrate system

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

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.

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*** (198) 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*** (199) 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*** (200) 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 ($I_{max\ peak}$) and the maximum steady state RMS current ($I_{max\ RMS}$) through the following formula: $I_{max\ peak} / I_{max\ RMS}$.

The **maximum** "Inrush Current Ratio" during a full operational cycle for detection systems ***shall*** (201) 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 ($I_{UNB\ Avg}$) – 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*** (202) 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*** (203) be verified and adjusted as needed during site acceptance.

Max Current Unbalance ($I_{UNB\ Max}$) – 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*** (204) 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*** (205) 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*** (206) 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.

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*** (207) 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 loses 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*** (208) be configured into the core system for automated monitoring and display of the current health and condition of the UPS.

APPENDIX E WBI REPORTS

1.0 FDRS REPORT DISPLAY

The WBI system ***shall*** (209) provide the reports listed in Table 1 below. Data reports (Reports 1, 2 and 3) ***shall*** (210) be viewable by calendar month and year (e.g., February 2008).

Table 1. WBI 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*** (211) 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*** (212) contain one record / row in the output table for each login session occurring in the date range. This report ***shall*** (213) 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)
WBIModelNo	Model Number of the WBI System	String (length = 8)
SiteCode	FAA Airport Code	String

Output Field	Description	Format
		(length = 3)
SubsiteCode	Machine Location	String (length = 20)

1.2 Event Report

An Event Report containing details of each system event ***shall*** (214) be provided. This report ***shall*** (215) consist of one row per event, and ***shall*** (216) provide data indicated in the following table. This report ***shall*** (217) be downloadable and be viewable on the IO Station monitor.

Output Field	Description	Format
MACHINE_ID	Identification Number of the WBI 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*** (218) 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*** (219) be downloadable and be viewable on the IO Station monitor.

Output Field	Description	Format
MACHINE_ID	Identification Number of the WBI System	String (length = 8)
User_ID	Identification login of the IO	String (length = 15)
AccessLevel	Access Control Level	String (length = 1)
Action	System action	Integer
ActionTime	Time action occurred	String

Output Field	Description	Format
		(length = 19)
ReportType	Report type	Integer
Downloaded	Was the file downloaded?	String (length=1)